Verifica della sicurezza di CURIAplus
Servizi del Parlamento

L'essenziale in breve

I Servizi del Parlamento (SP) coadiuvano l'Assemblea federale e i suoi organi nell'adempimento dei loro compiti. Oltre a fornire altri servizi, essi predispongono le applicazioni e i sistemi d'informazione per l'Assemblea federale e per i propri collaboratori. La Delegazione amministrativa è incaricata della direzione suprema dei SP. In una mozione accolta nel 2018, il Parlamento ha incaricato la Delegazione amministrativa di accelerare il processo di digitalizzazione dell'attività delle Camere e delle commissioni e di attribuire ai SP i mandati necessari a tal fine. In quest'ambito, i due progetti informatici CURIAplus e Cervin (Parlnet) sono di centrale importanza.

Già nel 2021 il Controllo federale delle finanze (CDF) ha verificato l'applicazione CURIAplus, Parlnet e la piattaforma di base Liferay.[1] In quell'occasione il CDF aveva constato diverse lacune. Di conseguenza, prima della messa in funzione di CURIAplus ha riesaminato la sicurezza informatica. Ha inoltre verificato lo stato di attuazione delle raccomandazioni formulate in precedenza.

Malgrado alcuni progressi nell'ambito della governance e dell'organizzazione permangono potenziali di miglioramento per entrambi i progetti CURIAplus e Parlnet, in particolare nei settori della sicurezza informatica, dei Service Level Agreement (SLA) e del backup dei dati.

La definizione di una governance e la riorganizzazione informatica sono efficaci

Nel mese di ottobre 2022 la Direzione dei SP ha posto in vigore la strategia di digitalizzazione dei Servizi del Parlamento. All'inizio del 2023 la Delegazione amministrativa ha posto in vigore le istruzioni concernenti la governance in relazione ai servizi digitali (disponibili solo in tedesco e francese). Nel settore dell'informatica i SP hanno effettuato un'ampia riorganizzazione passando al framework agile SAFe. Inoltre è stato potenziato l'effettivo del nuovo Comparto servizi digitali.

Le tematiche degli sviluppi futuri, come la nuova legge sulla sicurezza delle informazioni, o delle possibili conseguenze di un utilizzo di servizi cloud sono state affrontate in maniera proattiva e presentate alla Delegazione amministrativa.

I documenti relativi alla sicurezza devono essere rielaborati e approvati

Per la realizzazione del progetto, i SP si basano sulle direttive del framework SAFe. CURIAplus viene ancora gestito in conformità a HERMES e, una volta effettuati la messa in funzione e il completamento formale, si fonderà sulle direttive applicate a SAFe. Di conseguenza sono stati predisposti anche un'analisi del bisogno di protezione nonché un piano per la sicurezza delle informazioni e la protezione dei dati. Tuttavia non vi è stata alcuna approvazione formale di questi documenti.

[1] «Verifica del progetto CURIAplus» (n. della verifica 21310), disponibile sul sito Internet del CDF.

La protezione IT di base deve stabilire in maniera vincolante i requisiti minimi in ambito di sicurezza informatica dal punto di vista organizzativo, tecnico e del personale per tutti i mezzi informatici, inclusi i provvedimenti da adottare. Nel caso dei SP, non è definito in modo chiaro quali standard vengano presi in considerazione per la protezione di base e quali provvedimenti siano previsti.

La portata dei test sulla sicurezza informatica deve essere ampliata

Sono state condotte diverse verifiche esterne sulla sicurezza inerenti a Parlnet e alla piattaforma Liferay. Per ora non è stato ancora possibile risolvere tutte le problematiche emerse. È stata inoltre eseguita una revisione del codice sorgente, dalla quale non è emersa alcuna vulnerabilità critica. L'ampliamento della portata dei test ad altri sistemi periferici collegati, richiesto già nell'ultima verifica del CDF, non è stato attuato. Tuttavia, ciò è necessario per ottenere una visione globale della sicurezza informatica dei SP.

A causa di nuove installazioni, nel mese di aprile del 2023 non è stato possibile condurre una verifica esterna completa sulla sicurezza. I SP hanno commissionato la nuova esecuzione dei test per il mese di agosto del 2023, ovvero dopo la messa in funzione avvenuta nel mese di luglio. Secondo la raccomandazione del CDF, i test dovrebbero essere estesi ai sistemi periferici.

I SLA e i piani di emergenza devono essere definiti e coordinati tra di loro

Per poter reagire rapidamente in caso di malfunzionamento, le responsabilità dei vari fornitori devono essere chiarite e definite contrattualmente nei SLA. Mancano ancora i piani di emergenza sia per CURIAplus che per Parlnet. Inoltre, l'attuabilità delle misure di emergenza deve essere verificata regolarmente.

Occorre creare i backup esternalizzati e verificare la georidondanza

Poiché i SP sono stati classificati come infrastruttura critica, essi dovrebbero verificare la georidondanza in due centri di calcolo fisicamente separati. I SP dovrebbero perlomeno mettere a disposizione backup offline su un server remoto o su supporti esterni al proprio centro di calcolo.

Tre raccomandazioni risalenti alla verifica del 2021 risultano parzialmente attuate

I SP hanno fatto eseguire un'altra verifica sulla sicurezza e una revisione del codice. Tuttavia, la portata di tale verifica non è stata estesa come consigliato.

I documenti richiesti, i contratti e l'analisi dei rischi sono disponibili, ma tuttora in fase di elaborazione. Pertanto, le raccomandazioni risultano attuate solo parzialmente.

Testo originale in tedesco