CORTE DEI CONTI EUROPEA

IT

Comunicato stampa

Lussemburgo, 29 marzo 2022

Le istituzioni, organi e agenzie dell'UE devono essere più preparati in materia di cibersicurezza

Il numero di ciberattacchi contro organismi dell'UE è in rapido aumento. Il loro livello di preparazione in materia di cibersicurezza è variabile e complessivamente non commisurato alle crescenti minacce. Poiché tali organismi sono strettamente interconnessi, le debolezze di uno espongono gli altri a minacce per la sicurezza. Questa è la conclusione alla quale è giunta la Corte dei conti europea in una relazione speciale in cui viene esaminato il grado di preparazione degli organismi dell'UE di fronte alle minacce informatiche. La Corte raccomanda l'introduzione di norme vincolanti in materia di cibersicurezza e un aumento delle risorse della squadra di pronto intervento informatico (CERT-UE). La Commissione europea dovrebbe inoltre, secondo la Corte, promuovere una maggiore cooperazione tra gli organismi dell'UE, mentre la CERT-UE e l'Agenzia dell'Unione europea per la cibersicurezza dovrebbero concentrarsi maggiormente su quegli organismi dell'UE che hanno minore esperienza nella gestione della cibersicurezza.

Il numero di incidenti significativi registrati dagli organismi dell'UE è più che decuplicato tra il 2018 e il 2021 e il telelavoro ha aumentato considerevolmente i potenziali punti di accesso per gli aggressori. Gli incidenti significativi sono generalmente causati da attacchi informatici sofisticati, che generalmente includono l'uso di nuovi metodi o tecnologie, e le indagini su tali incidenti e il ripristino del normale funzionamento possono richiedere settimane, se non addirittura mesi. Un esempio è stato il ciberattacco sferrato nei confronti dell'Agenzia europea per i medicinali (EMA), che ha portato alla divulgazione di dati sensibili poi manipolati per minare la fiducia nei vaccini.

"*Le istituzioni, organi e agenzie dell'UE sono obiettivi interessanti per potenziali aggressori, in particolare per i gruppi in grado di attuare attacchi altamente sofisticati ed invisibili a fini di ciberspionaggio o altre finalità illecite*" ha dichiarato Bettina Jakobsen, il Membro della Corte responsabile dell'audit. "*Tali attacchi possono comportare significative implicazioni politiche, nuocere alla reputazione generale dell'UE e minare la fiducia nelle sue istituzioni. L'UE deve fare di più per proteggere i propri organismi*".

La principale constatazione della Corte è che le istituzioni, organi e agenzie dell'UE non sono sempre adeguatamente protetti dalle minacce informatiche. Non adottano un approccio uniforme alla cibersicurezza, non sempre applicano i controlli essenziali e le buone pratiche in materia e non

Lo scopo del presente comunicato stampa è illustrare i messaggi principali della relazione speciale della Corte dei conti europea. Il testo integrale della relazione è disponibile su eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg

E: press@eca.europa.eu @EUAuditors eca.europa.eu

forniscono sistematicamente formazione a tale riguardo. Le risorse destinate alla cibersicurezza variano notevolmente e alcuni organismi dell'UE spendono notevolmente meno rispetto ai propri omologhi di dimensioni analoghe. Anche se i diversi livelli di cibersicurezza potrebbero essere teoricamente giustificati dai diversi profili di rischio di ciascuna organizzazione e dai diversi livelli di sensibilità dei dati trattati, la Corte sottolinea che le carenze della cibersicurezza in un organismo dell'UE possono esporre numerose altre organizzazioni a minacce informatiche (gli organismi dell'UE sono strettamente interconnessi tra loro e spesso anche con organizzazioni pubbliche e private negli Stati membri).

La Squadra di pronto intervento informatico (CERT-UE) e l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) sono le due principali entità che forniscono sostegno in materia di cibersicurezza. Tuttavia, a causa delle risorse limitate e della priorità attribuita ad altri ambiti, non sono state in grado di fornire tutto il sostegno di cui gli organismi dell'UE necessitano. A giudizio della Corte, un altro difetto riguarda la condivisione delle informazioni: ad esempio, non tutti gli organismi dell'UE diffondono tempestivamente comunicazioni sulle vulnerabilità e sugli incidenti significativi di cibersicurezza di cui sono stati vittime o che possono avere ripercussioni su altri organismi.

Informazioni sul contesto

Attualmente non esiste un quadro giuridico riguardante la sicurezza delle informazioni e la cibersicurezza nelle istituzioni, nelle agenzie e negli organismi dell'UE. Questi non sono soggetti alla normativa UE più generale in materia di cibersicurezza, ossia la direttiva NIS (*network and information security*) del 2016, né alla relativa proposta di revisione, la direttiva NIS2. Non vi sono inoltre informazioni complete sugli importi spesi dagli organismi dell'UE per la cibersicurezza. Nel luglio 2020 la Commissione ha pubblicato una comunicazione sulla strategia dell'UE per l'Unione della sicurezza per il periodo 2020-2025, che contiene "norme comuni in materia di sicurezza delle informazioni e sicurezza informatica per l'insieme degli organismi dell'UE". Nella strategia dell'UE in materia di cibersicurezza per il decennio digitale, pubblicata nel dicembre 2020, la Commissione annunciava la presentazione di un regolamento contenente norme comuni sulla cibersicurezza per tutti gli organismi dell'UE. Proponeva inoltre la creazione di una nuova base giuridica per la CERT-UE al fine di consolidarne mandato e finanziamenti.

La relazione speciale 05/2022 "*Cibersicurezza delle istituzioni, degli organi e delle agenzie dell'UE: il livello complessivo di preparazione non è commisurato alle minacce*" è disponibile sul sito Internet della Corte. La Corte ha evidenziato inoltre le sfide insite in un'efficace politica dell'UE in materia di cibersicurezza in un documento di riflessione del 2019.

Contatto stampa

Ufficio stampa della Corte: press@eca.europa.eu

- Claudia Spiti – e-mail: claudia.spiti@eca.europa.eu – cell. (+352) 691 553 547
- Vincent Bourgeais – e-mail: vincent.bourgeais@eca.europa.eu – cell. (+352) 691 551 502
- Damijan Fišer damijan.fiser@eca.europa.eu – cell. (+352) 621 552 224