Università degli Studi di Palermo
Area Sistemi Informativi di Ateneo

Al personale Docente e Ricercatore

Al personale TAB

Oggetto: rischio di Trasferimento dei Dati Strategici dell'Ateneo

Con la crescente dipendenza dalle tecnologie informatiche e la diffusione del lavoro remoto, è necessario affrontare con serietà la questione della sicurezza dei dati strategici dell'Ateneo. Il presente documento intende evidenziare il rischio associato al trasferimento di tali dati dai sistemi informativi centrali alle postazioni personali, che non potendo adottare gli stessi criteri di sicurezza dei server centrali, presentano un rischio significativo di esfiltrazione e compromissione dei dati.

In conformità con il Regolamento Generale sulla Protezione dei Dati (GDPR), l'Ateneo è legalmente tenuto a garantire la sicurezza e la riservatezza dei dati personali e strategici di tutta la comunità, inclusi carriere studenti, dati sui voti, dati del personale in servizio e altre informazioni sensibili.

Il trasferimento di tali dati verso postazioni personali, sicuramente non dotate di criteri di sicurezza adeguati, presenta i seguenti rischi:

1. **Esfiltrazione dei Dati**: le postazioni personali possono essere soggette a minacce esterne come malware, phishing e attacchi informatici mirati, che possono consentire a malintenzionati di accedere ai dati sensibili e trasferirli illecitamente al di fuori dell'ambiente protetto dei server centrali dell'Ateneo.
2. **Compromissione della Sicurezza**: le postazioni personali potrebbero non essere soggette allo stesso livello di protezione e monitoraggio continuo dei server centrali, aumentando il rischio di accessi non autorizzati e violazioni della sicurezza che potrebbero compromettere l'integrità e la riservatezza dei dati.
3. **Violazione del GDPR**: il trasferimento dei dati strategici dell'Ateneo verso postazioni personali potrebbe violare le disposizioni del GDPR in materia di protezione dei dati personali e comportare conseguenze legali e finanziarie per l'Ateneo.

Al fine di mitigare questi rischi e garantire la sicurezza dei dati strategici dell'Ateneo, si raccomanda:

Viale delle Scienze Ed. 11 – 90128 Palermo
segreteria.sia@unipa.it - pec: areasia@cert.unipa.it
http://www.unipa.it

1. **Politiche di Accesso e Controllo**: implementare rigorose politiche di accesso e controllo dei dati, limitando l'accesso solo al personale autorizzato e monitorando attentamente le attività di utilizzo dei dati.
2. **Formazione e Sensibilizzazione**: garantire adeguata formazione ed informazione a tutti i soggetti che utilizzano dati rilevanti per l'Ateneo, al fine di sensibilizzare il personale sull'importanza della sicurezza dei dati e sulle migliori pratiche per proteggere le informazioni sensibili.
3. **Criptaggio dei Dati**: utilizzare tecniche di criptaggio per proteggere i dati durante il trasferimento e lo stoccaggio, garantendo che siano inaccessibili agli utenti non autorizzati.
4. **Evitare il trasferimento dei dati**: evitare il trasferimento dei dati da host protetti verso dispositivi che non offrono le stesse garanzie di protezione. Monitorare il trasferimento dei dati dai vari dispositivi.
5. **Rispettare le Policy di sicurezza**: periodicamente riesaminare e verificare le politiche e le procedure di sicurezza dei dati per garantirne la corretta applicazione.

La sicurezza dei dati strategici dell'Ateneo è una responsabilità condivisa da tutti noi. Con l'adozione di misure preventive adeguate e la consapevolezza dei rischi associati al trasferimento dei dati verso postazioni personali, possiamo proteggere l'integrità e la riservatezza delle informazioni sensibili dell'Ateneo.

Cordiali Saluti.

Il Responsabile del Servizio Speciale Prevenzione della Corruzione e Trasparenza, Privacy e Regolamenti di Ateneo	Il Data Protection Officer	Il Dirigente dell'Area Sistemi Informativi di Ateneo
Avv. Maurizio Faraci	Dott. Antonino Pollara	Dott. Riccardo Uccello
Firmato digitalmente da: Maurizio Faraci Data: 22/04/2024 15:49:53	Firmato digitalmente da: Antonino Pollara Data: 22/04/2024 17:07:45	Firmato digitalmente da: Riccardo Uccello Data: 23/04/2024 08:22:48