UNIMORE
UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

PIANO DI SICUREZZA INFORMATICA

2024-2025

dell'Università di Modena e Reggio Emilia

Approvato dal CdA in data
21.12.2023

PIANO DI SICUREZZA INFORMATICA 2023-2025

dell'Università di Modena e Reggio Emilia

Premessa

L'Università degli Studi di Modena e Reggio Emilia intende affrontare in maniera organica il tema della sicurezza delle informazioni e della cybersecurity, proseguendo un percorso avviato nell'anno 2017 con l'adeguamento alle misure minime di sicurezza AgID e proseguito negli anni successivi con il censimento delle applicazioni e l'istituzione del Gruppo Sicurezza ICT e del Computer Security Incident Response Team (CSIRT).

La Direzione Sistemi Informativi e Assicurazione Qualità ha svolto un'attività di CyberSecurity Maturity Assessment per valutare il livello di sicurezza dell'Ateneo, identificare i gap rispetto ai framework e alle best practice internazionali e definire una roadmap di implementazione.

È stato quindi predisposto un piano di implementazione di misure di sicurezza, per il biennio 2024 e 2025.

L'obiettivo è quello di aumentare la resilienza dell'Ente ad eventi avversi che comportano una potenziale perdita di dati e interruzione di servizi, attraverso l'implementazione di tecnologie e servizi ed attraverso l'applicazione di misure organizzative.

La governance della sicurezza informatica dell'Ateneo

Il responsabile della sicurezza informatica dell'Ateneo è il Responsabile della Transizione Digitale (RTD).

L'RTD dell'Università degli Studi di Modena e Reggio Emilia è la Dott.ssa Paola Michelini – nominata con delibera del Consiglio di Amministrazione nella seduta del 16 gennaio 2023. L'RTD nello svolgimento del proprio incarico si avvale di un Ufficio dirigenziale denominato Ufficio della Transizione Digitale (Ufficio RTD), i cui compiti sono elencati all'art. 17 CODICE DELL'AMMINISTRAZIONE DIGITALE - D.lgs 82/2005 e s.m.i.

L'Ufficio della Transizione Digitale (Ufficio RTD) dell'Ateneo è la Direzione Sistemi Informativi ed Assicurazione della Qualità. All'interno dell'Ufficio RTD è presente un'unità operativa "Ufficio Reti, Sistemi, Fonia e Cybersecurity" che coordina le attività tecniche in materia di sicurezza informatica.

L'Ufficio della Transizione Digitale (Ufficio RTD) dell'Ateneo si avvale della collaborazione e del supporto tecnico e specialistico del CRIS - unità operativa di sicurezza informatica - coordinata da Prof. Mirco Marchetti (DIEF), Dott. Mauro Andreolini (FIM), Prof. Luca Ferretti (FIM).

L'Ateneo ha sottoscritto un protocollo d'intesa per la prevenzione e contrasto dei crimini informatici sui sistemi informativi "critici" dipendenti da UniMORE con la Polizia di Stato - Centro Operativo per la Sicurezza Cibernetica Emilia-Romagna (Rif. deliberazione del Senato Accademico Repertorio n. 18/2023 Prot n. 46538 del 15/02/2023 e deliberazione del Consiglio di Amministrazione n. 42/2023 Prot n. 63315 del 27/02/2023.

Misure di sicurezza

Gestione backup e servizi di disaster recovery - business continuity

Analisi dell'attuale infrastruttura di backup e di erogazione dei servizi al fine di valutarne la robustezza in caso di eventi avversi o disastrosi, dovuti a malintenzionati, a guasti o malfunzionamenti, o eventi naturali.

Progettazione ed implementazione di una soluzione di backup "air gapped" che permetta il ripristino dei dati in caso di ransomware che colpisca anche i sistemi di backup.

Predisposizione di un piano di Business Continuity/Disaster Recovery a partire dai tempi di Recovery Time Objective (RTO) e Recovery Point Objective (RPO) individuati attraverso l'attività di Business Impact Analysis (BIA).

Attivazione della Multi Factor Authentication

La Multi Factor Authentication (MFA) aggiunge ai meccanismi di autenticazione basati su username e password un secondo fattore di autenticazione che utilizza un canale diverso rispetto a quello utilizzato per l'accesso, che permette di proteggere l'accesso ai sistemi che la utilizzano anche in caso di furto di credenziali.

La MFA verrà attivata il prima possibile sugli accessi remoti tramite VPN. Questo tipo di accesso è infatti utilizzato frequentemente dai criminali informatici come primo accesso alle reti delle vittime utilizzando credenziali valide sottratte attraverso attacchi di phishing o trovate sul dark web e rappresenta quindi una misura di sicurezza urgente.

In un secondo momento la MFA verrà estesa per proteggere l'accesso ad altri sistemi critici, per esempio all'accesso da parte degli amministratori di sistema. Verrà quindi utilizzata nell'ambito della piattaforma di Privileged Access Authentication.

Misure di sicurezza di rete

Rafforzare la sicurezza della rete attraverso

- la predisposizione di funzionalità avanzate sul firewall (es. funzionalità di SSL inspection);
- l'introduzione di sistemi Web Application Firewall (WAF);
- la segmentazione della rete dell'Ateneo;
- l'introduzione di sistemi Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)/Security Information and Event Management (SIEM) per la gestione di eventi di sicurezza sugli endpoint - piattaforma di Endpoint Detection and Response (EDR), eventi di rete (raccolti dalla piattaforma di Network Detection and Response (NDR)), Log di sistema (raccolti dalla piattaforma SIEM).

Soluzioni in Cloud

Potenziamento della strategia di migrazione al Cloud nelle modalità Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e **Software as a service (SaaS)**

Servizi di sicurezza

Servizio di Incident Response Team e Cyber Threat Intelligence

La finalità del servizio di Incident Response Team è quella di intervenire rapidamente a fronte di un attacco informatico andato a buon fine. L'attività dell'IRT consiste nell'analizzare le dinamiche di attacco che hanno portato alla compromissione degli asset dell'organizzazione, i vettori d'attacco che sono stati usati per fare breccia sui sistemi e le vulnerabilità che sono state sfruttate per eseguire azioni illecite sui server coinvolti, fornendo quindi indicazioni su come sanare le vulnerabilità che hanno consentito agli attaccanti di perpetrare azioni illecite sui sistemi e incrementare di fatto il livello globale di sicurezza dell'organizzazione.

Il servizio di Cyber Threat Intelligence (CTI) ha come obiettivo il monitoraggio delle allerte di sicurezza provenienti da varie fonti (OSINT e CLOSINT) al fine di identificare, classificare e notificare minacce di sicurezza informatica.

Vulnerability Assessment + Penetration Test (Infrastrutturale e Web App)

Il Vulnerability Assessment effettua una fotografia della infrastruttura e verifica eventuali falle nella sua configurazione: questo consente una valutazione dello stato dei sistemi di sicurezza implementati su reti, macchine o applicazioni aziendali, con l'obiettivo di rilevare eventuali carenze di protezione rispetto ad elenchi di vulnerabilità tecnologiche note.

Il Penetration Test è un'indagine sperimentale sulla sicurezza di un computer o di una rete, volta a individuare vulnerabilità che potrebbero essere sfruttate in caso di tentativo di accesso non autorizzato e a testare i controlli che dovrebbero proteggere i computer e le reti da tali tentativi. Il test è articolato sostanzialmente in due fasi:

- l'esplorazione dei presidi di sicurezza del sistema oggetto di verifica;
- tentativo di violare quei presidi e di penetrare il sistema stesso (c.d. attacco).

Formazione specialistica per dirigenti e personale IT

L'attività ha l'obiettivo di consentire al personale dell'Ateneo di accrescere la consapevolezza e la responsabilizzazione degli utenti in merito alle tematiche di sicurezza e privacy, ognuno per il proprio ruolo, contribuendo a rendere più sicuro l'intero ambiente di lavoro, attraverso iniziative in aula rivolte agli addetti IT ai dirigenti non IT, agli addetti alla cybersecurity.

Campagna di phishing simulato/awareness

Le campagne di phishing etico, intese come campagna di sensibilizzazione interna che simula attacchi reali, vengono usate per:

- verificare e migliorare la consapevolezza dei dipendenti di una società sui temi della sicurezza
- riconoscere e fronteggiare questo tipo di attacchi
- proteggere il proprio business evitando possibili infezioni da malware
- difendere i propri sistemi da eventuali programmi spia
- salvaguardare i documenti più strategici
- distinguere e-mail lecite da e-mail nocive
- adottare le dovute contromisure in modo che altri colleghi non ne siano vittime
- rafforzare le difese di sicurezza indipendentemente dalla tecnologia utilizzata (p. es. i filtri antispam non sempre sono adeguati).

Il progetto di formazione si ispira alla necessità di sensibilizzare il dipendente circa il rischio informatico e all'importanza di dare il giusto peso all'aspetto della sicurezza delle informazioni aziendali. Obiettivi del progetto di formazione sulla consapevolezza, sono:

- Rendere consapevole il dipendente del rischio di Cyber Crime
- Innalzare il livello di attenzione alla riservatezza e alla cura dei dati dell'organizzazione
- Verificare e migliorare le capacità di rilevamento in caso di attacco
- Monitorare la capacità di risposta del dipendente e dell'organizzazione

Revisione dell'implementazione delle misure minime di sicurezza AGID

Le misure minime di sicurezza ICT emanate dall'AgID nel 2017, sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti. Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale e utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.

L'adeguamento alle misure minime è a cura del responsabile dell'RTD, come indicato dall'art. 17 del CAD. La versione corrente è stata approvata in data 6/6/2019.