Settembre 2021

Misure di sicurezza relative alle infrastrutture di Trentino Digitale S.p.A.

Premessa

La sicurezza informatica è un aspetto sempre più critico e complesso, sia per la crescente digitalizzazione che per l'aumento del numero di attacchi informatici e della loro sofisticazione.
I rischi derivano principalmenti dai seguenti elementi:

- possibili vulnerabilità nelle infrastrutture e nei sistemi di erogazione dei servizi digitali;
- postazioni di lavoro e comportamento degli utenti finali.

Trentino Digitale S.p.A., società in-house della Provincia Autonoma di Trento:

- dispone e gestisce le infrastrutture provinciali di rete del territorio della Provincia Autonoma di Trento, in primis quella geografica in fibra ottica ed eroga servizi di connettività e di accesso ad Internet a favore degli Enti pubblici soci e del Sistema Trentino;
- dispone e gestisce le infrastrutture di due data center classificati nel "Gruppo A" di AgID (Agenzia per l'Italia Digitale)[1] dal punto di vista di requisiti di affidabilità e sicurezza, ed eroga servizi di data center e cloud a favore degli Enti pubblici soci e del Sistema Trentino;
- ha conseguito la qualificazione Cloud Service Provider (CSP) di AgID[2] ed eroga servizi cloud disponibili sul Cloud Marketplace di AgID;
- dispone di un NOC (Network Operation Center) e di un SOC (Security Operation Center) per il monitoraggio e la gestione del funzionamento e della sicurezza;
- dispone di una organizzazione per la gestione della sicurezza delle informazioni ed è certificata ISO 27001 estesa ai controlli aggiuntivi ISO 27017 (sicurezza dei dati in Cloud) e ISO 27018 (privacy dei dati personali in Cloud) e anche ISO 22301 a garanzia della continuità operativa dei servizi;

[1] Circolare n.1 del 14 giugno 2019
https://www.agid.gov.it/sites/default/files/repository_files/circolare_1_agid_2019_id_2.pdf
[2] Circolari n. 2 e n.3 del 9 aprile 2018
https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/181151234430O__OCircolare+2-2018_Criteri+per+la+qualificazione+dei+Cloud+Service+Provider+per+la+PA.pdf

- è impegnata costantemente nell'aggiornamento delle misure di sicurezza e dei processi al fine di garantire un adeguato livello di sicurezza sia in termini di prevenzione che di reazione.

Sicurezza perimetrale

Trentino Digitale S.p.A. dispone di meccanismi di sicurezza, in continua evoluzione ed aggiornamento che includono:

- strumenti di protezione di rete (cosiddetti Firewall per regolare il traffico in entrata e in uscita secondo regole stabilite) con funzioni di rilevazione delle intrusioni (cosiddetti IPS; *Intrusion Prevention System*) e relativa policy;
- strumenti di protezione dei sistemi e dei servizi di Data Center: Firewall e relative policy anche a livello di servizio applicativo;
- strumenti di protezione di una parte consistente dei server che contribuiscono alla protezione anche da attacchi malware/ransomware;
- strumenti e sistemi di monitoraggio della rete, dei Data Center e delle principali componenti applicative;
- verifiche periodiche dei sistemi di erogazione dei principali servizi esposti su Internet (Vulnerability Assessment e Penetration Test).

Tutto il traffico Internet gestito da Trentino Digitale, ad eccezione del traffico consegnato attraverso peering BGP (*Border Gateway Protocol*), è sottoposto a regole firewall che, oltre a garantire la sicurezza della rete permettono di "loggare" il traffico secondo quanto disposto dalla normativa e quindi di monitorare e rilevare, a cura del SOC, anche in tempo reale, eventuali anomalie o criticità.

Sicurezza dei servizi di connettività

Trentino Digitale S.p.A gestisce la rete geografica in fibra ottica (denominata Telpat) che copre il territorio della Provincia di Trento, realizzata con tecnologia MPLS (*Multiprotocol Label Switching*) e suddivisa logicamente in aree, attraverso il meccanismo di VRF (*Virtual Routing and Forwarding*). Le varie VRF della rete MPLS terminano sui *Firewall* che garantiscono la comunicazione tra le aree, oppure tra sottoaree, attraverso apposite policy diversificate. Tale suddivisione della rete in aree e sottoaree, ne garantisce la segmentazione del traffico e quindi la sicurezza. Tutti i nodi principali della rete geografica in fibra ottica sono interconnessi in doppia via su percorsi fisici distinti e sono dotati di facility con meccanismi in grado di garantire la continuità dei servizi.

Trentino Digitale S.p.A. gestisce inoltre numerose reti informatiche locali LAN (*Local Area Network*) degli Enti del Sistema Trentino dove, in caso di necessità, vengono implementati meccanismi di segmentazione del traffico attraverso VLAN (*Virtual Local Area Network*) e apparati Firewall piuttosto che liste di accesso ACL (*Access-List*) definite opportunamente. Tali meccanismi possono essere utili ad esempio per diversificare la gestione delle postazioni di lavoro all'interno della stessa LAN.

Sicurezza dei servizi di Data Center

La gestione delle reti interne LAN ai Data Center avviene sempre attraverso l'implementazione di segmentazioni della rete con tecnologie VLAN terminate sui Firewall. In alcune VLAN vengono implementati, ove è necessario, meccanismi di "host isolation" come ulteriore misura di protezione all'interno della stessa LAN.
I Data Center di Trentino Digitale sono anche nodi principali della rete geografica in fibra ottica, sono pertanto interconnessi in doppia via su percorsi fisici distinti e sono dotati di facility con meccanismi in grado di garantire la continuità dei servizi.

I sistemi di Trentino Digitale S.p.A. deputati all'erogazione dei servizi di data center e cloud sono tutti oggetto di monitoraggio costante e prevedono meccanismi di backup secondo opportune policy, diversificate a seconda delle esigenze di ciascun servizio, con duplicazione e conservazione delle copie di dati su due diverse locazioni geografiche. Inoltre, per specifici servizi vengono realizzati, ove è richiesto, meccanismi di disaster recovery e di business continuity utilizzando i data center di Trentino Digitale o di soggetti terzi.

Sicurezza degli accessi fisici

Trentino Digitale dispone di un processo per la gestione e il controllo degli accessi fisici garantendo un costante controllo delle autorizzazioni concesse con particolare riguardo alle aree maggiormente critiche. In particolare gli accessi ai nodi della rete geografica in fibra ottica e ai Data Center sono oggetto di specifiche policy restrittive, di un controllo basato su sistemi di videosorveglianza e un monitoraggio da parte di una apposita control room attiva H24.

SOC (Security Operation Center)

Trentino Digitale dispone di un SOC, attivo H24 7x7 365, che eroga anche servizi agli Enti pubblici del territorio trentino, con un controllo continuo degli eventi di sicurezza anche attraverso l'utilizzo di un sistema SIEM (*Security Information and Event Management*) e di un sistema di EndPoint Protection. Le attività del SOC permettono di prevenire, rilevare e gestire eventuali anomalie di sicurezza anche grazie alla collaborazione con la Polizia Postale di Trento e le segnalazioni del CSIRT nazionale (*Computer Security Incident Response Team - Italia*).