SIELCO: PANORAMICA SULLA SICUREZZA

Ver. 1.1 - Aggiornamento del 20/11/2021

SIELCO fornisce servizi datacenter IAAS, SAAS e housing puntando sulla sicurezza del dato e della sua gestione.

ISO 27001

SIELCO è certificata ISO 27001 accreditamento riconosciuto internazionalmente per la gestione sicura delle informazioni. SIELCO, come azienda certificata ISO 27001, dà ai clienti la possibilità di fare audit sui propri sistemi. Il costo dell'audit verrà quantificato in funzione del tempo e del numero di servizi. La richiesta di audit deve avvenire tramite PEC.
SIELCO risponderà con una quantificazione economica, comunque non superiore a 1.000,00 € per singolo audit. All'accettazione verrà concordata la data dell'audit e le relative procedure.

ISO 27017/27018

SIELCO è in fase di certificazione ISO 27017 & ISO 27018 internazionalmente riconosciute per la sicurezza dei servizi cloud (per servizi cloud si intendono sia quelli erogati da SIELCO che da terze parti il cui tramite è SIELCO).

DATA CENTER

SIELCO collabora con partner accuratamente selezionati.
I servizi core sono erogati tramite l'infrastruttura presente nel datacenter DATA4 CAMPUS di Cornaredo. Il datacenter ha una certificazione ANSI TIER IV (per consultare la lista completa delle certificazioni visitare il sito: hiips://www.data4group.com/it/data -centers-certifications/).
I servizi di terze parti sono erogati dai datacenter Microsoft o Amazon certificati ISO 27001 e ISO 27017 & ISO 27018.

SICUREZZA DEI DATI E CIFRATURA

SIELCO fornisce un servizio MSP (Managed Service Provider) gestito completamente o parzialmente. I clienti in fase di sottoscrizione del servizio possono selezionare il grado di sicurezza da attivare tra cui, per esempio, la MFA (multifactor authentication), la retention, la periodicità del backup, la cifratura dei dati, ecc. Le tecnologie integrate nei nostri servizi sono riepilogate nella tabella seguente, in cui è anche indicato se è attivabile la cifratura:

SGBOX	LIBRAESVA ANTISPAM	VEEAM BACKUP	ICEWARP MAIL SERVER	MICROSOFT RDS	TSPLUS	TEAMSYSTEM	ARXIVAR	NAV
OK	NO	OK	CONSIGLIAMO MIGRAZIONE SU 365	OPZIONALE	OPZIONALE	OPZIONALE	OPZIONALE	OPZIONALE

SIGLA	DROPBOX	MICROSOFT 365	KAPSERSKY	CLOUDALLY	EXCLAIMER	WASABI	LUCIDLINK	ECOS
OPZIONALE	OK	OPZIONALE	OPZIONALE	OK	CIFRATURA IN TRANSIT	OK	OK	OPZIONALE

BACKUP

Per i servizi di produzione erogati dal datacenter ad esclusione del backup in cloud e del DR – che sono già una copia del dato di produzione – SIELCO applica una policy di backup 3-2-1: sono previste almeno 3 copie del dato su almeno 2 supporti diversi tra cui 1 copia off-site. La copia off-site è dislocata presso un datacenter olandese a cui è stata applicata una policy di “immutability” (il dato non può essere modificato per 30 gg neanche dagli amministratori di sistema). In questo modo il dato è protetto da ransomware, dagli hacker, dal furto di identità e da possibili manomissioni dolose. In fase di sottoscrizione del servizio il cliente può selezionare una retention e una periodicità personalizzata. I backup hanno una retention di base di 5 giorni. I backup sono cifrati di default con 256-bit AES con una chiave a 256-bit e con CBC-mode e sono verificati in automatico dal software e, su richiesta, a campione dai tecnici SIELCO. Il ripristino dipende dalla quantità di dati e dalla fonte (datacenter locale o remoto). Non essendo il backup un disater recovery, viene garantita la resilienza del dato, ma non il tempo di rispristino che, se non contrattualizzato diversamente, potrebbe protrarsi fino a 10 giorni lavorativi. SIELCO è disponibile a fare dei test di recovery a pagamento se richiesto dal cliente tramite i consueti canali commerciali. Per i servizi di produzione rivenduti da SIELCO ma erogati da terzi (es. Microsoft 365) non è garantito il backup salvo non sia previsto contrattualmente dal fornitore terzo o salvo aver sottoscritto con SIELCO un apposito contratto.

CREDENZIALI UTENTE

In fase di attivazione del servizio SIELCO crea le credenziali per usufruirne in accordo con il cliente. Per la creazione, modifica e/o cancellazione di ulteriori credenziali con ruoli amministrativi durante la durata del contratto è necessaria una richiesta nel portale di ticketing (hiips://help.sielco.it) da parte del rappresentante legale dell'azienda o di un suo delegato. È onere del cliente segnalare a SIELCO modifiche alle deleghe. Se non diversamente specificato tra i delegati rientrano anche gli interlocutori abituali di SIELCO come, per esempio, l'IT manager o l'incaricato che si occupa di informatica all'interno dell'azienda. Utente e password verranno inviati tramite due canali di comunicazione diversi (es. utente via mail, password via sms).

Per la gestione dei diritti di accesso degli utenti (es: accesso a una cartella condivisa), il cliente può fare richiesta tramite il portale di ticketing hiips://help.sielco.it

GESTIONE DELLE PASSWORD

L'assegnazione delle password avviene in modo sicuro come specificato nel capitolo "Credenziali utente". Il cliente ha la possibilità nei portali dei servizi sottoscritti di modificare la propria password. Essendo comunque servizi gestiti è sempre possibile richiedere l'aiuto dell'helpdesk di SIELCO via portale di ticketing all'indirizzo hiips://help.siel co.it

AUTENTICAZIONE A PIÚ FATTORI

In fase di sottoscrizione dei servizi è possibile richiedere l'autenticazione a più fattori ove supportate. Le tecnologie integrate nei nostri servizi sono riepilogate nella tabella seguente, in cui è anche indicato se è attivabile l'autenticazione a più fattori:

SGBOX	LIBRAESVA ANTISPAM	VEEAM BACKUP	ICEWARP MAIL SERVER	MICROSOFT RDS	TSPLUS	TEAMSYSTEM	ARXIVAR	NAV
OK	INTEGRABILE CON 365	ENFORCED PER I RIVENDITORI, OPZIONALE PER I CLIENTI	OPZIONALE	OPZIONALE	OK	OPZIONALE	OPZIONALE	OPZIONALE

SIGLA	DROPBOX	MICROSOFT 365	KAPSERSKY	CLOUDALLY	EXCLAIMER	WASABI	LUCIDLINK	ECOS
NO	OPZIONALE	OPZIONALE	OPZIONALE	OPZIONALE	OPZIONALE	OPZIONALE	OZPIONALE	OPZIONALE CON TSPLUS

FORMAZIONE

SIELCO si impegna a effettuare formazione a tutti i dipendenti sulla cybersicurezza. Attraverso una piattaforma web, i dipendenti e i collaboratori di SIELCO hanno a disposizione diversi percorsi di formazione a seconda della preparazione personale e del tipo di dato trattato.

SITI & APPLICAZIONI WEB

Per i siti e le applicazioni web pubblicate con domini SIELCO (sielco.it, si-cloud.it, ecc) viene utilizzato il protocollo HTTPS con certificati pubblici rilasciate da CA (Certification Authority) riconosciute. Per i siti e le applicazioni web pubblicate con domini non di proprietà di SIELCO è possibile richiedere, da parte del cliente, un certificato pubblico a pagamento.

VULNERABILITY ASSESSMENT

SIELCO assegna periodicamente delle VA (Vulnerability Assessment) alla propria infrastruttura e applica le remediation in base alla valutazione del rischio. I clienti possono richiedere un servizio VA opzionale a pagamento sulle proprie VM o sui propri apparati fisici.

SICUREZZA PERIMETRALE

SIELCO protegge la propria infrastruttura e quella dei clienti tramite:

- appliance firewall con funzioni di
    - ✓ IDS/IPS (Intrusion Detection System/Intrusion Prevention System)
    - ✓ funzioni ATP (Advanced Threat Protection)
- antivirus perimetrale
- opzionalmente, a pagamento, è possibile attivare anche:
    - ✓ Reverse proxy
    - ✓ WAF (Web Application Firewall)

LOG

SIELCO raccoglie i log dell'infrastruttura (Hypervisor, Switch, Firewall, ecc.) e li correla tramite una piattaforma ad hoc. Questa gestione consente sia di intervenire automaticamente che di segnalare al personale SIELCO eventuali possibili anomalie. SIELCO raccoglie anche i logo di accesso degli amministratori alle VM dei clienti. È possibile estendere questa funzionalità opzionalmente, a pagamento, anche sulle macchine del cliente tramite l'apposito servizio proposto da SIELCO.

I log, salvo diversamente specificato, sono mantenuti con queste retention:

- ✓ Eventi: 3 mesi
- ✓ Log RAW: 6 mesi
- ✓ Log per i clienti col contratto SIEM: 365 giorni
- ✓ Backup dei log 365: giorni

COLLEGAMENTO DA REMOTO

Per i collegamenti alla propria infrastruttura SIELCO mette a disposizione dei clienti dei canali sicuri, tra cui HTTPS e VPN (Virtual Private Network).

Questi canali vengono cifrati in accordo con il cliente sulla base dei requisiti tecnici richiesti.

Esistono altri strumenti che possono venire proposti in aggiunta o in alternativa a seconda delle esigenze specifiche del cliente.

PATCHING

SIELCO utilizza dei sistemi di "patching" automatici, semi automatici o manuali per la propria infrastruttura.

Il "patching" viene effettuato ad intervalli periodici o in base all'uscita di vulnerabilità particolarmente rilevanti.

È possibile estendere il servizio di "patching" anche sulle macchine dei clienti tramite un servizio opzionale a pagamento.

DIVULGAZIONE DEI DATI

SIELCO si impegna con il CLIENTE a non effettuare alcuna divulgazione dei dati salvo che ciò sia:

- ✓ Richiesto e concordato contrattualmente con il cliente del servizio cloud.
- ✓ Sia richiesto espressamente dalle forze dell'ordine. In questo caso, salvo divieto delle forze dell'ordine stesse, la divulgazione sarà tempestivamente notificata al cliente del servizio cloud.
- ✓ SIELCO si impegna a tenere un registro in cui inserire quali dati siano stati divulgati, a chi e quando.

TRASPORTO DEI DATI

Quando il trasporto di dati è effettuato con apparati di proprietà SIELCO, SIELCO si impegna a utilizzare supporti cifrati (come, per esempio, NAS con volumi cifrati). SIELCO darà evidenza della cifratura dell'apparato apponendo sull'apparato stesso un adesivo di colore ROSSO.

Se il trasporto è effettuato con apparati di proprietà del cliente, il cliente può chiedere al personale SIELCO di cifrare i dati se gli apparati forniti supportano tale funzione.

Se il trasporto è effettuato digitalmente, SIELCO si impegna ad utilizzare canali cifrati, come, per esempio, VPN, HTTS, FTPs, SSH, ecc.

CLOCK

Tutti i servizi SIELCO sono sincronizzati con NTP server pubblici, in particolare con: *.ntp.pool.org e ntp*.inrim.it

FORENSICS

Attività di "computer forensic" o attività di supporto alla "computer forensic", non sono comprese. SIELCO si rende disponibile a seguito di richiesta del cliente a fornire un preventivo per tali attività ed eventualmente ad indicare degli esperti nel campo a cui il cliente si può rivolgere.

CHIAVI DI CIFRATURA

SIELCO gestisce le chiavi di cifratura dei propri servizi nel seguente modo:

- ✓ SERVIZI GESTITI DA SIELCO

  In questo caso le chiavi di cifratura sono conservate e gestite da SIELCO. SIELCO le conserva all'interno del proprio perimetro informatico e si preoccuperà di regolare l'accesso e il salvataggio delle chiavi. È possibile, da parte dei clienti, richiedere un audit per la verifica delle procedure interne.

- ✓ SERVIZI GESTITI DAL CLIENTE (Es: cloud storage)

  Le chiavi di cifratura possono essere generate dal cliente, se è autonomo, oppure generate da SIELCO. Se generate da SIELCO verranno poi spedite al cliente tramite canali sicuri (Onedrive o Dropbox). In ogni caso SIELCO **NON** conserverà copia delle chiavi e sarà onere del cliente custodirle in modo adeguato. In caso di smarrimento della chiave di cifratura, né SIELCO, né l'eventuale fornitore terzo possono recuperare i dati.