Il Titolare ed i suoi Co-Titolari hanno intrapreso un Piano di Adeguamento biennale per la migrazione di tutto il Sistema Privacy e Protezione dei Dati (SPPD) aziendale in recepimento della riforma del Regolamento Europeo per la Protezione dei Dati Personali (GDPR) ratificato in Italia come Reg.679/2016. Dal 2023 sono state recepite e implementate anche le nuove direttive UE per la CyberSecurity.

POLITICA PRIVACY 4.0

Compliance Art.25 ICT in Azienda

Questo documento viene divulgato trasparentemente per descrivere gli adempimenti di compliance coordinati dal DIP prescritti dall'Art. 25 del Reg.679/2016 successivamente aggiornati dal Dlg. 101/2018 (sinteticamente Privacy 4.0). La redazione dei contenuti è validata dal RIP che supervisiona la implementazione curata dagli ADS, RET e ADAT (v. web MSPPD). Gli Standard di riferimento per la ricognizione di audit sono: ISO27002, ITIL/CoBIT e CSF ENISA (v. web MSPPD)

SICUREZZA: MISURE FISICHE

Politiche e contromisure di resilienza a tutela di apparati e strumentazione utilizzata all'interno del sito della sede operativa della organizzazione così come all'esterno nel caso di uso di dispositivi BYOD di proprietà aziendale

SICUREZZA: MISURE LOGICHE

Politiche e contromisure di funzionalità e integrità digitale e informatica a livello di configurazione e dotazione software per postazioni di lavoro e tutti i dispositivi informatici della LAN aziendale e del suo perimetro tecnologico

SICUREZZA: MISURE ORGANIZZATIVE

Politiche e contromisure per aggiornamento, istruzione, educazione digitale, consapevolezza tecnologica e formazione preventiva di tutti gli addetti aziendali per minimizzare rischio di avversità dovute a risorse umana. Tutte le figure privacy sono designate con compiti e istruzioni specifiche per le proprie funzioni aziendali in relazione alla Privacy 4.0

Sommario dei Contenuti

- ***Continuità di rete e antincendio***
- ***Piano di formazione e affiancamento***
- ***Stoccaggio dati di Sistema e dati di business***
- ***Stoccaggio per il Disaster Recovery***
- ***Difesa di Network perimetrale***
- ***Difesa Cyber: malware e ransomware***
- ***Segregazione e isolamento trattamenti ICT***
- ***Licensing, Patch Management e Paternità IT***

Riferimenti Manuale SPPD aziendale digitale:

Piano di Audit ICT annuale; Modulo Audit per WEB; Disciplinare di Sicurezza IT; Audit annuale per la Valutazione dei Rischi IT; Check-List ricognizione ICT CoBIT Library Based

Continuità di rete e anti-incendio

Il primo requisito classificato durante la Analisi Dei Rischi ICT è quello di dotare gli apparati informatici dell'armadio tecnico di un Sistema Tampone di Alimentazione Elettrica.

Un *blackout* della corrente elettrica è sempre possibile e quando non si tratta di un problema locale di elettrocuzione e/o corto, può sempre dipendere dalla rete esterna. In queste circostanze è stata fatta una valutazione di priorità di copertura dimensionando la capacità tampone adeguata ai Server di Rete, al Firewall e all'unità NAS della LAN a mezzo unità UPS.

Tutti gli apparati protetti sono *shock-sensitive*, quindi tramite cavo USB o RJ45 con l'unità UPS intraprendono uno shut-down conservativo pilotato da dispositivo UPS

Gli ambienti con installati armadi tecnici e/o quadri di distribuzione IT e in prossimità di dispositivi critici per il Sistema Informativo il Responsabile del sistema di *Safety* RSSP ha provveduto a alloggiare estintori a schiuma regolarmente verificati da fornitore qualificato

Piano di Formazione e affiancamento

Con la migrazione dal Sistema Privacy conforme al Codice Privacy al Regolamento Europeo per la Protezione dei Dati Personali il paradigma della informazione e della formazione in ambito informatico è ulteriormente evoluto. Dovendo adottare misure adeguate allo Stato dell'Arte tecnologico la formazione è stata pianificata secondo una calendarizzazione periodica, è stata verbalizzata sistematicamente seguendo prassi e procedure scritte, è stata differenziata in ragione delle diverse tipologie di trattamento con strumenti informatici e per i Soggetti Autorizzati si è ricorso anche a sessioni di affiancamento pratico.

In tutti i casi sono state previste anche sessioni di seminari frontali soprattutto in occasione della introduzione di nuove tecnologie e/o modifiche dei Sistemi Informativi.

Tutti i soggetti operanti anche solo temporaneamente in azienda (visitatori, clienti e/o stagisti), sono stati istruiti sulle norme comportamentali del Disciplinare Interno ICT. Dove necessario oltre alle istruttorie verbali preliminari, soggetti Terzi (stagisti, sessioni a clienti per demo di prodotti) e/o semplici Destinatari (docenti e corsisti ospitati per lezioni/seminari) ricevono e sottoscrivono modulo di informativa e NDA (vincolo di riservatezza).

Segregazione e isolamento dei trattamenti ICT

Le attività di business della azienda coinvolgono diverse tipologie di addetti che utilizzano in modo differenziale le dotazioni delle infrastrutture ICT che oltre ad essere fisicamente distinte in ambienti confinati, sono "informaticamente" configurate per un accesso selezionato e specifico. Il Titolare ha fornito supporto economico e dato mandato a figure dedicate (RIP, ADS e RET) per la progettazione, la implementazione e il mantenimento continuo di un Sistema Informativo basato su misure logiche e organizzative basate su livelli di sicurezza per il controllo di Accesso (ACL).

Il Sistema Informativo intramurale è basato sulla tecnologia MS AD-DS (Active Directory & Directory Services) multi livello. Questo servizio centralizza in un Domain Server dedicato la gestione di segregazione e isolamento dei livelli di condivisione di tutte le risorse informatiche e di accesso ai loro contenuti.

La stessa Server Station svolge anche un servizio di DHCP statico cosi da accoppiare al livello di controllo delle autenticazioni con credenziali personali, quello autorizzativo grazie alla identificazione univoca della coppia valori *MAC address* e IP dei dispositivi HW (Es. Stampanti di rete multi funzione, scanner, BYOD).

La architettura identificativa distribuita viene utilizzata per tutte le procedure di *escalation* ACL basate su credenziali per l'accesso, il controllo e la modifica di tutti gli apparati di Network e Storage condivisi. In sintesi sia Firewall perimetrale che unità NAS di LAN sono sincronizzati con il Server AD-DS permettendo una associazione univoca operatore-risorsa in tutta l'infrastruttura ICT.

Stoccaggio dati di Sistema e dati di business

ADEGUAMENTO HW - Nel raggiungimento della completa migrazione tecnologica ICT del SPPD aziendale la organizzazione ha acquisito una unità di Network Area Storage (NAS) centrale per tutte le utenze intramurali. Tale NAS basato su un sistema Linux *embedded* è stato configurato con una alberatura ereditata dal Domain Server AD-DS talché fosse disegnata la stessa architettura logica di condivisione delle risorse.

Pertanto il disegno distribuito di ACL è stato associato alle aree funzionali della società, e di conseguenza, degli operatori autorizzati al trattamento dei dati di business e degli applicativi rispettando tutte le credenziali autenticative/autorizzative ratificate nelle Politiche e le POS di Sistema DP.

AUTOMAZIONE COPIE - Tutti i dati e le informazioni di business correnti sottostanno a procedute automatiche di copie di sicurezza. Sono state definite tre tipologie di copie di sicurezza: copie ombra, repliche speculari e volumi storicizzati. Questi ultimi sono estesamente descritti nel paragrafo successivo "*Stoccaggio per il Disaster Recovery*".

Il NAS pertanto contiene copie e repliche implicite alla tecnologia RAID5 ma anche un ulteriore livello di sicurezza via automazione *batch/bash* che ridonda repertori cifrati e compressi su base temporale

DATI DI SISTEMA - Oltre ai dati di business lo stoccaggio di sicurezza viene calendarizzato anche con procedure manuali che conservano le immagini dei Sistemi Operativi dei Server e delle stazioni di lavoro critiche nelle quali si ricorre alla virtualizzazione. I formati di immagine conservati sulle unità NAS (eventualmente HD rimovibili e/o trasportabili) sono: VHD/VHDS, HyperV, Vbox, ISO6600

LOG MANAGEMENT - La completa struttura di "segregazione e isolamento" delle identità digitali "*inbreed"*, è infine monitorata con una altrettanto completo "*Log Management*" quale adempimento prescrittivo del Regolamento Privacy e Protezione dei Dati Personali. Peraltro, la collezione dei *log* della *lan* è stata realizzata con una architettura distribuita di tipo *Push* dalla periferia al Server seguendo un metodo Readiness Forense (tecnicamente "instrumentazione"). In estrema sintesi, tutte le postazioni di lavoro sono continuamente sincronizzate (*hooked*) da processi silenti e trasparenti sul PC degli operatori; questi automatismi "sorvegliano" i contenuti e gli eventi del sistema propagando sul Server centralizzato i Log (protocollo *SysLog* su NAS).

Sempre in ambito di stoccaggio automatico, non solo le stazioni di lavoro ma anche il Firewall perimetrale usa lo stesso canale di sicurezza sul NAS per tutti i log di Network. Questo implica che il tracciamento digitale viene realizzato anche per tutte le comunicazioni (eventi o attività) entranti dalla WAN (vedi sotto "*Difesa perimetrale di Network*" e "*Difesa Cyber: malware e ransomware*").

Stoccaggio per il Disaster Recovery

Nel paragrafo precedente è stato descritto l'approccio sistemico e centralizzato alla sicurezza nello stoccaggio delle informazioni aziendali basato sull'apparato di NAS. Questa tecnologia è affidabile e potente come contromisura di sicurezza locale, tuttavia, e per quanto sia remota, esiste sempre la possibilità del "cigno nero". Se cioè accade un evento avverso di portata disastrosa (allagamento, incendio ecc.), insieme alla compromissione e/o la perdita della strumentazione informatica si rischia il danno alla periferica del NAS che si trova fisicamente negli stessi ambienti *on premise*.

Tutti gli standard di sicurezza indirizzano il problema della *Disaster Recovery* verso l'adozione di repliche *alter sito* dei Sistemi Informatici e/o delle informazioni di contenuti digitali.

In questo contesto la organizzazione ricorre a un terzo livello di repliche sincronizzate (già introdotti sopra come "*Repertori Storicizzati*"). Essenzialmente, tutte le Repliche periodiche dei dati sul NAS a loro volta vengono copiati in Cloud. Questa volta la comunicazione utilizza i protocolli S-FTP, RSync e RTRR (nativo della unità NAS)

Per i dati di sistema (configurazioni, immagini OS, Vaults credenziali ecc.) lo stoccaggio di sicurezza viene calendarizzato anche con procedure manuali che conservano le immagini dei Sistemi Operativi dei Server e delle stazioni di lavoro critiche nelle quali si ricorre alla virtualizzazione. I formati di immagine conservati sulle unità NAS (eventualmente HD rimovibili e/o trasportabili) sono: VHD/VHDS, HyperV, Vbox, ISO6600

Difesa di Network perimetrale

Sicurezza HW: La sicurezza perimetrale è ovviamente basata sulla configurazione di un Firewall UTM dimensionato per il controllo di flusso delle comunicazioni TCP-IP. Oltre al filtraggio di ***appliances*** anti-virus, AP, anti-*ransomware*, anti-*spam*, *content filtering*, VPN *tunneling* SSL e WAN/DMZ L2TL over IPSec per citare le caratteristiche principali, i nostri informatici hanno configurato politiche di DHCP *static Table* (già menzionate sopra).

Per i punti di accesso di WI-FI si sono scelte tecniche di sezionamento e isolamento di *subnet* e di rotazione periodica della chiave di cifratura *WPA2-PSK*. In nessun caso sono persistite configurazioni di connessioni automatiche con *HotSpot* esterni ai *range* di DHCP statico.

Sicurezza SW – un ulteriore livello di controllo è l'audit sistematico per la precoce rilevazione di attacchi ed intrusioni per prevenire violazioni informatiche come previsto dagli adempimenti mandatori del Provv. sul "***Data Breach***" (IDS/IPS e DLP). A compendio si sono configurate procedure e regole di re-indirizzamenti e re-instradamenti NAT/PAT (*Network* e/o *Port addressing*) custom per le comunicazioni interne/esterne o vice versa dirette verso servizi standard come ad esempio protocolli di Database Server, flussi di RDP e teleassistenza.

Difesa Cyber: misure anti-malware e anti Ransomware

Oltre alle misure per le minacce Cyber ai flussi di comunicazione delle informazioni descritti in precedenza, la organizzazione ha curato misure più specifiche per gli attacchi di *social engineering* che colpiscono aggirando le difese di perimetro di LAN (vedi sopra). La prima contro-misura "specifica" è diretta all'elemento critico del fattore umano

con la formazione agli operatori già descritta sopra, in seconda istanza si è operato sul SW di "instrumentazione" già citato. La consapevolezza IT (*Readiness & awareness*) traversa tutti i livelli degli operativi della azienda.

Il SW anti virus è presente su tutte le postazioni di elaborazione ed agisce non solo sui contenuti di signature dei *bytecodes* delle basi aggiornate quotidianamente ma anche sui flussi delle comunicazioni "socket" a livello di Sistema Operativo di ogni stazione di lavoro. Questo controllo di flusso intercetta anche i contenuti della navigazione web e delle attività di posta elettronica (in entrata e in uscita).

Accanto al livello basale dell'Antivirus, nella azienda si sono adottate misure addizionali basate su *appliance* di *community* internazionali quali ad esempio i *plug-in* per navigatore internet WOT e Ghostery e processi di background specifici per il Ransomware basati su "*behavioral analisys*" e "*crypto library interceptor*" (Cybereason, CyberSight RamStopper, BitDefender A-R e Kaspersky Lab A-R.

Licensing, Patch Management e Paternità

Per sua vocazione di business e in quanto reseller di licenze SW, la nostra organizzazione ha sempre curato sia dal punto di vista regolatorio che della difesa del Diritto d'Autore e il rispetto delle Proprietà Intellettuali di Marchi e Brevetti, le politiche di Licensing e Patch Management.

Per la validazione dei programmi/codici proprietari gli ADS interni usano anche tecniche di validazione hashing e certificati utilizzando l'applicazione di gestione certificati proprietari Kleopatra basata sulla Certificate Authority OpenPGP. I certificati sono utilizzati per le attività che sfruttano i protocolli di trasmissione HTTPS,S_FTP e FTP-S o sono destinate alle procedure di stoccaggio per la cifratura (RSync/RTRR vedi sopra)

Tutti i contratti di licenza d'uso delle piattaforme di sviluppo SW, OSs, applicazioni gestionali e middleware ERP/CRM sono stipulati per l'usufrutto interno di sistema e/o la rivendita di servizi terzi da e per la clientela.

Sia personale commerciale che sviluppatori sono qualificati (accreditati e/o certificati) con i brand delle piattaforme SW di prodotto.

Autenticazione, repudiabilità, contraffazione e paternità di contenuti digitali (sia codice SW che documenti ufficiali) sono livelli di sicurezza critici per alcuni processi di gestione dei dati Personali quando gli Interessati sono i Clienti di commessa. Il Titolare ed i suoi co-titolari, adottano per tutte le informazioni soggetti ad usufrutto/disseminazione soggette a potenziali violazioni di atti riservati e/o brevettuali e/o vincolati da accordi d'impresa misure ulteriori di sicurezza informatica. Le tecniche implementate alla bisogna, sono scelte, documentate e manutenute dagli ADS della organizzazione e seguono *frameworks* di standard internazionali quali NIS-CSF , ENISA, ITIL e **CoBIT library** all'interno della infrastruttura on-premise e CSA e OWASP per le are web e CC. I certificati di marca temporale, firma digitale e hashing sono quelle descritti per i protocolli di trasmissione.

Versione 2024

DIP / ADS

……