# SECURITY SPRINT 30 GIORNI

## Piano Operativo di Cybersicurezza per Aziende

## INTRODUZIONE

Questo Security Sprint è progettato per Aziende che vogliono migliorare concretamente la propria postura di sicurezza in 30 giorni, con investimenti contenuti e risultati misurabili.

**Principi guida:** - Azioni concrete, non teoria - Budget-friendly - Impatto immediato - Sostenibile nel tempo

## SETTIMANA 1: MAPPATURA E CONSAPEVOLEZZA

**Obiettivo:** Sapere cosa proteggere

### Giorno 1-2: Inventario degli Asset Digitali

**Cosa fare:** - Elencare tutti i sistemi critici (server, cloud, software gestionali) - Identificare dove sono conservati i dati sensibili - Mappare chi ha accesso a cosa

**Strumento:** Foglio Excel semplice con colonne: Asset | Criticità (1-5) | Responsabile | Backup Presente (Sì/No)

**Output:** Lista prioritaria di ciò che va protetto per primo

### Giorno 3-4: Audit delle Password

**Cosa fare:** - Verificare quanti dipendenti usano password deboli - Identificare account condivisi (da eliminare!) - Controllare se ci sono password scritte o salvate in chiaro

**Azione immediata:** - Imporre password di almeno 12 caratteri - Implementare password manager aziendale (es. Bitwarden / Keepass)

### Giorno 5: Verifica Backup

**Cosa fare:** - Controllare se i backup esistono davvero - Testare il ripristino di UN file da backup - Verificare che i backup siano offline o protetti

**Regola 3-2-1:** 3 copie, 2 supporti diversi, 1 off-site

### Giorno 6-7: Assessment Iniziale

**Cosa fare:** - Compilare un questionario di autovalutazione (vedi appendice) - Identificare le 3 vulnerabilità più critiche - Definire priorità per le prossime settimane

**Tool gratuito:** CIS Controls Self Assessment Tool (CIS CSAT)

## SETTIMANA 2: PROTEZIONE BASE

**Obiettivo:** Alzare le difese fondamentali

### Giorno 8-9: Autenticazione Multi-Fattore (MFA)

**Cosa fare:** - Attivare MFA su tutti gli account critici (email, banking, cloud, gestionale) - Priorità: email aziendale e accessi amministrativi - Formare il team sull'uso

**Perché è cruciale:** L'MFA blocca il 99,9% degli attacchi automatizzati

**Tool consigliati:** Microsoft Authenticator, Google Authenticator, o Probator

### Giorno 10-11: Aggiornamenti di Sicurezza

**Cosa fare:** - Verificare che tutti i sistemi operativi siano aggiornati - Aggiornare software aziendali critici - Attivare aggiornamenti automatici dove possibile

**Checklist:** - [ ] Windows/macOS aggiornato - [ ] Antivirus aggiornato (e attivo!) - [ ] Browser aggiornati - [ ] App aziendali aggiornate

### Giorno 12-13: Firewall e Antivirus

**Cosa fare:** - Verificare che firewall sia attivo su tutti i dispositivi - Confermare che antivirus enterprise sia installato ovunque - Testare le scansioni programmate

**Per PMI:** Windows Defender + firewall nativo sono spesso sufficienti se ben configurati

### Giorno 14: Sicurezza della Rete Wi-Fi

**Cosa fare:** - Cambiare password Wi-Fi predefinita - Usare WPA3 o almeno WPA2 - Creare rete separata per ospiti - Nascondere SSID se possibile

## SETTIMANA 3: FATTORE UMANO

**Obiettivo:** Trasformare i dipendenti in prima linea di difesa

### Giorno 15-16: Policy Chiare e Comprensibili

**Cosa fare:** - Creare una "Policy di Sicurezza su 1 Pagina" - Regole essenziali in linguaggio semplice - Farla firmare a tutti

**Contenuti minimi:** - Gestione password - Uso dispositivi personali - Email sospette - Cosa fare in caso di incidente

### Giorno 17-18: Mini-Training Anti-Phishing

**Cosa fare:** - Sessione formativa di 30 minuti con esempi reali - Mostrare email di phishing reali ricevute - Spiegare i segnali d'allarme

**Elementi da riconoscere:** - Senso di urgenza ("Agisci subito!") - Link sospetti (passare il mouse senza cliccare) - Mittenti strani - Richieste insolite

**Pratica:** Simulazione phishing amichevole (avvisare prima!)

### Giorno 19-20: Processo di Segnalazione

**Cosa fare:** - Creare canale dedicato per segnalare anomalie (email, chat, telefono) - Nominare un "referente sicurezza" interno - Garantire che non ci siano ritorsioni per segnalazioni

**Messaggio chiave:** "È meglio 100 falsi allarmi che un attacco non segnalato"

### Giorno 21: Test di Consapevolezza

**Cosa fare:** - Quiz rapido per verificare l'apprendimento - Premiare chi ottiene punteggio alto - Sessione di recupero per chi fatica

**Gamification:** Classifica amichevole, piccoli premi

## SETTIMANA 4: CONSOLIDAMENTO E CONTINUITÀ

**Obiettivo:** Rendere la sicurezza sostenibile

### Giorno 22-23: Piano di Risposta agli Incidenti

**Cosa fare:** - Creare checklist: "Cosa fare se..." - Ricevo email sospetta - Computer infetto - Dati cancellati - Accesso negato (possibile ransomware)

**Contatti di emergenza:** - IT interno o fornitore - Legale - Polizia Postale (se necessario) - Backup provider

### Giorno 24-25: Contratti e Fornitori

**Cosa fare:** - Verificare clausole di sicurezza nei contratti con fornitori IT - Controllare SLA e copertura assicurativa - Valutare cyber-insurance (almeno preventivo)

**Domande ai fornitori:** - "Come proteggete i nostri dati?" - "Avete certificazioni di sicurezza?" - "Cosa succede in caso di breach?"

### Giorno 26-27: Audit di Chiusura

**Cosa fare:** - Ripetere assessment iniziale del Giorno 6-7 - Misurare i miglioramenti - Documentare cosa è stato fatto

**Metriche di successo:** - % sistemi con MFA attivo - % dipendenti formati - Tempo medio di backup testato - Vulnerabilità critiche risolte

### Giorno 28-29: Roadmap Trimestrale

**Cosa fare:** - Pianificare prossimi 90 giorni - Identificare investimenti da fare - Programmare training di refresh

**Elementi della roadmap:** - Certificazioni da ottenere (es. ISO 27001 se rilevante) - Tool da implementare - Audit esterni da pianificare

### Giorno 30: Celebration & Commitment

**Cosa fare:** - Comunicare i risultati a tutta l'azienda - Celebrare il traguardo (anche simbolicamente) - Impegnarsi pubblicamente alla continuità

**Messaggio del CEO:** "In 30 giorni abbiamo reso la nostra azienda più sicura e più competitiva"

## MANUTENZIONE CONTINUA

### Checklist Mensile (30 minuti)

- ☐ Verificare backup recenti
- ☐ Controllare log antivirus
- ☐ Aggiornare software critici
- ☐ Revisione accessi utenti

### Checklist Trimestrale (2 ore)

- ☐ Test ripristino backup
- ☐ Refresh formazione dipendenti
- ☐ Audit password deboli
- ☐ Revisione policy

### Checklist Annuale (1 giornata)

- ☐ Assessment completo
- ☐ Aggiornamento piano di risposta incidenti
- ☐ Valutazione nuove minacce
- ☐ Considerare audit esterno

## INVESTIMENTI CONSIGLIATI

### Budget Minimo (< €2.000/anno)

- Password manager: €100-300
- MFA: gratuito (Google/Microsoft Authenticator/Probator)
- Training online: €200-500
- Backup cloud: €300-600
- Antivirus enterprise: €500-1.000

### Budget Medio (€2.000-10.000/anno)

- Tutto quanto sopra +
- Firewall gestito: €1.500-3.000
- Cyber insurance: €1.000-5.000
- Consulenza esterna (1-2 giorni): €1.500-3.000
- Tool di monitoraggio: €1.000-2.000

### ROI Atteso

- Riduzione rischio breach: 70-80%
- Tempo risposta incidenti: -60%
- Conformità normativa: raggiunta
- Opportunità business: +25% (gare che richiedono certificazioni)

## APPENDICE A: QUESTIONARIO DI AUTOVALUTAZIONE

**Punteggio: 0 = No, 1 = Parzialmente, 2 = Sì**

### Gestione Accessi

- ☐ Tutti gli account hanno password complesse (12+ caratteri)?
- ☐ È attivo MFA su account critici?
- ☐ Gli accessi vengono revocati immediatamente quando qualcuno lascia l'azienda?
- ☐ Esiste una lista aggiornata di chi ha accesso a cosa?

### Backup e Continuità

- ☐ Backup automatici sono configurati?
- ☐ I backup vengono testati regolarmente?
- ☐ Esiste un backup offline o off-site?
- ☐ C'è un piano documentato di disaster recovery?

### Aggiornamenti e Protezione

- ☐ Sistemi operativi sono aggiornati?
- ☐ Antivirus è installato e aggiornato su tutti i dispositivi?
- ☐ Firewall è attivo?
- ☐ Software viene aggiornato regolarmente?

### Formazione e Policy

- ☐ I dipendenti hanno ricevuto training sulla sicurezza nell'ultimo anno?
- ☐ Esiste una policy di sicurezza scritta e comunicata?
- ☐ C'è un processo chiaro per segnalare incidenti?
- ☐ I dipendenti sanno riconoscere email di phishing?

### Rete e Dispositivi

- ☐ La rete Wi-Fi aziendale è protetta con password forte?
- ☐ Esiste una rete separata per ospiti?
- ☐ I dispositivi mobili aziendali hanno misure di sicurezza?
- ☐ Vengono usati VPN per connessioni remote?

**PUNTEGGIO TOTALE: ____ / 40**

- **0-15:** Rischio Alto - iniziare immediatamente lo Sprint
- **16-28:** Rischio Medio - buona base, miglioramenti necessari
- **29-36:** Rischio Basso - ottimo lavoro, mantenere e perfezionare
- **37-40:** Eccellente - considerare certificazioni formali

## APPENDICE B: TEMPLATE EMAIL DI SEGNALAZIONE

**Oggetto:** [SECURITY] Segnalazione Anomalia

Ho notato quanto segue: - **Cosa:** [descrivere l'evento sospetto] - **Quando:** [data e ora] - **Dove:** [sistema/dispositivo coinvolto] - **Chi:** [persone coinvolte se rilevante] - **Azioni intraprese:** [cosa ho fatto/non fatto]

**Urgenza:** [ ] Bassa [ ] Media [ ] Alta

## APPENDICE C: CHECKLIST PRIMO GIORNO POST-INCIDENTE

### Azioni Immediate (prima ora)

- ☐ Isolare il sistema compromesso (disconnettere da rete)
- ☐ NON spegnere il dispositivo (può cancellare prove)
- ☐ Fotografare lo schermo con il telefono
- ☐ Avvisare il referente sicurezza
- ☐ Cambiare password account critici da dispositivo pulito

### Azioni Successive (entro 24 ore)

- ☐ Documentare tutto per iscritto
- ☐ Verificare integrità backup
- ☐ Informare clienti/partner se dati esposti (GDPR)
- ☐ Considerare denuncia Polizia Postale
- ☐ Coinvolgere legale se necessario

### Non Fare

- ✗ Pagare riscatti ransomware prima di consultare esperti
- ✗ Cancellare prove
- ✗ Nascondere l'incidente (peggiora le conseguenze)
- ✗ Tentare riparazioni "fai da te" su sistemi critici

## RISORSE UTILI

### Tool Gratuiti Consigliati

- **Keepass:** Password manager open source
- **Have I Been Pwned:** Verifica se email è stata compromessa
- **CIS Controls:** Framework di sicurezza
- **Cybersecurity Framework NIST:** Linee guida USA (ottimo riferimento)

### Contatti Utili Italia

- **Polizia Postale:** www.commissariatodips.it
- **CERT-AgID:** Incidenti sicurezza PA e privati
- **Garante Privacy:** Per violazioni dati personali
- **ACN (Agenzia Cybersicurezza Nazionale):** www.acn.gov.it

### Formazione Continua

- **SANS Cyber Access:** Tutorial gratuiti
- **Cybrary:** Corsi base gratuiti
- **Google Security Training:** Materiale didattico gratuito

## NOTE FINALI

**Questo Security Sprint non è:** - Una certificazione formale - Una garanzia contro tutti gli attacchi - Un sostituto di consulenza professionale per casi complessi

**Questo Security Sprint è:** - Un punto di partenza concreto - Una base solida di buone pratiche - Un percorso accessibile per Aziende con risorse limitate - Un vantaggio competitivo misurabile

**Ricorda:** La sicurezza perfetta non esiste. L'obiettivo è essere più sicuri di ieri e più preparati di gran parte della concorrenza.

**Prossimi passi suggeriti dopo i 30 giorni:** 1. Considerare ISO 27001 se opportunità business lo richiedono 2. Audit esterno annuale da professionista certificato 3. Espandere formazione con simulazioni avanzate 4. Valutare penetration test per sistemi critici 5. Implementare SIEM (Security Information Event Management) se scala aziendale lo giustifica

*"La sicurezza non è una destinazione, è un viaggio. Questo Sprint è il vostro primo passo."*

**Buon lavoro!**