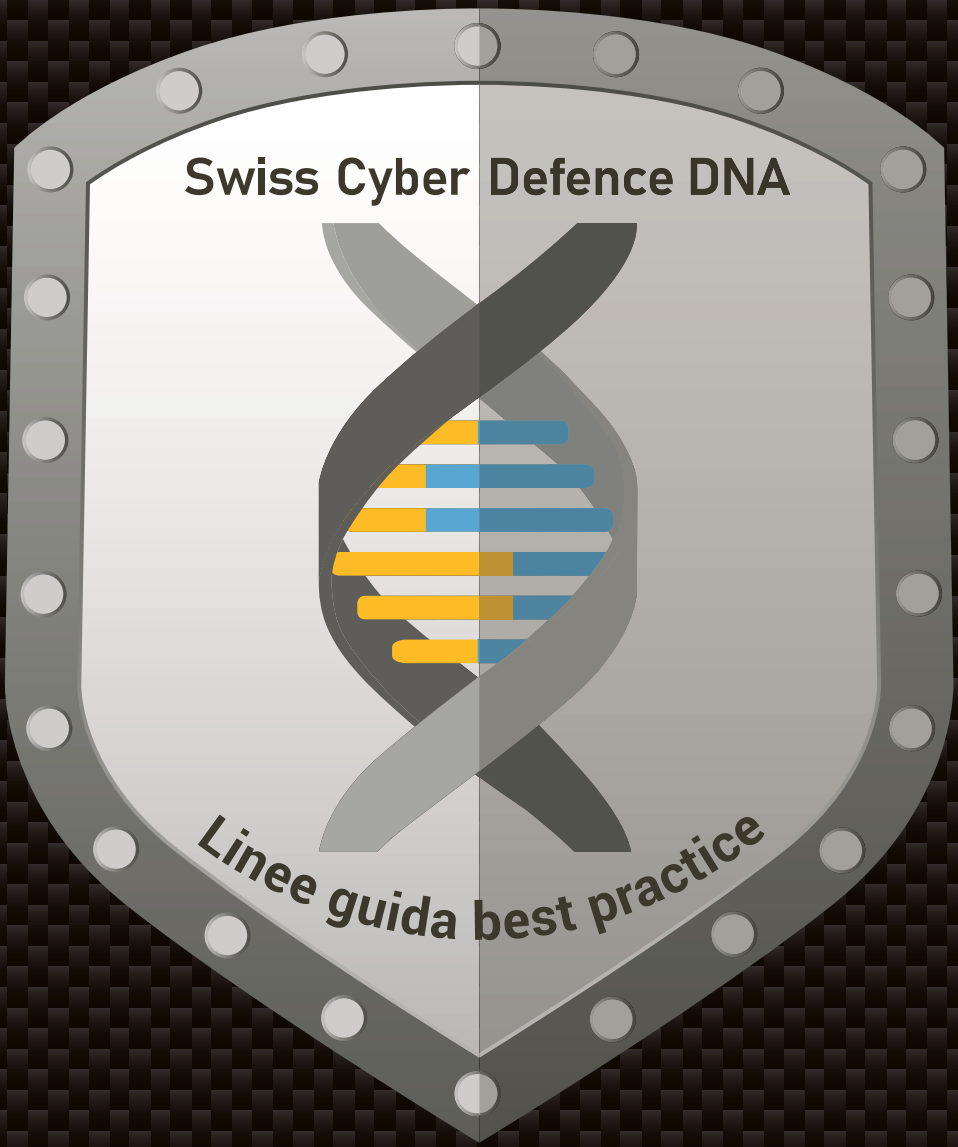
Protezione dai ricatti per le PMI



L'essenziale per sopravvivere nell'era digitale

Swiss Cyber Defence DNA

L'essenziale per sopravvivere nell'era digitale

Swiss Cyber Defence DNA (SCD-DNA) è un documento contenente linee guida per la vostra PMI con cui potete difendervi in modo semplice ed efficace dai rischi della cyber-criminalità e da gravi danni finanziari. Rendete la vita difficile ai cyber-criminali, in modo da non essere ricattabili. SCD-DNA è un'iniziativa di MOUNT10 AG con la partecipazione di diversi partner industriali.

Il seguente elenco di misure tiene conto allo stesso modo dei settori di responsabilità organizzazione e tecnologia della vostra PMI.

Misura n. 1 – Protezione dei dati aggiornata e non modificabile / backup in sola lettura

Garantite la sopravvivenza della vostra azienda, come nel caso dell'airbag in auto

- ☐ Definire un responsabile dell'attuazione e della verifica
- ☐ Assicurare il salvataggio esterno del backup
- ☐ Processo di backup automatizzato e in sola lettura, incl. cifratura
- ☐ Se quanto sopra non è possibile: separare il medium di backup dalla rete ed effettuare il salvataggio offline

Misura n. 2 – Protezione globale e aggiornata dai software dannosi

La vostra prima difesa, come una sicura porta d'ingresso a casa

- ☐ Sensibilizzare e formare il personale nella gestione di e-mail, siti web, password ecc.
- ☐ Proteggere in modo globale e capillare dal malware apparecchi terminali, server, servizi cloud ed e-mail
- ☐ Limitare l'esecuzione delle macro; installare filtri internet e antispam

Misura n. 3 – Proteggere le reti e gli accessi da remoto

I vostri reparti di difesa per bloccare in modo selettivo gli accessi non autorizzati

- ☐ Formare il personale e i fornitori per l'accesso da remoto
- ☐ Suddividere le reti in zone mediante il firewall, in modo da isolare importanti settori aziendali
- ☐ Proteggere ulteriormente l'accesso da remoto mediante l'autenticazione a due fattori (ad es. codice SMS)

Misura n. 4 – Mantenere sempre aggiornati hardware e software

La garanzia per un IT sicuro ed efficiente

- ☐ Definire un responsabile per la gestione e la verifica periodica delle licenze / degli aggiornamenti
- ☐ Sostituire i sistemi obsoleti conformemente all'analisi dei rischi e proteggere fisicamente i sistemi attuali (ad es. accesso al server)
- ☐ Utilizzare soltanto sistemi operativi e applicazioni aggiornati
- ☐ Isolare i vecchi sistemi dalla rete

Misura n. 5 – I collaboratori e i rispettivi ruoli

La vostra autoprotezione riducendo il tutto all'essenziale

- ☐ Definire in un concetto dei ruoli le autorizzazioni necessarie a ogni collaboratore
- ☐ Verificare e delimitare anche i diritti di accesso della direzione
- ☐ Stabilire le regole relative alle password per i collaboratori
- ☐ Abbinare i ruoli definiti con i diritti di accesso e delimitarli

Misura n. 6 – Definire i processi d'emergenza

La vostra protezione nei casi d'emergenza: un piano chiaro anziché l'improvvisazione

- ☐ Stabilire un'organizzazione d'emergenza e i relativi processi; informare tutti i collaboratori
- ☐ Verificare regolarmente ruoli e processi e testare il feedback dei dati
- ☐ Utilizzare tecnologie indipendenti, per poter accedere ai documenti anche nei casi d'emergenza (ad es. istruzioni in caso d'emergenza, cartelle, cloud o soluzione mobile)

Ulteriori informazioni su scd-dna.ch

Promotori

TREND MICRO

MOUNT10
SWISS DATA DEFENCE

Hewlett Packard Enterprise

COMPASS SECURITY

SOPHOS
Cybersecurity evolved.

atrete
IT consultants

swisscom

Microsoft

CISCO

LA POSTA

helvetia

Mecenati, Partecipanti & Partner web

BOLTONSHIELD

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

n|w Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

LEFIMATIK
Lehrlingsfirma für Mediamatik
Ein Projekt der Bägli ICT AG

Consegnato da

Ulteriori informazioni su
kmuschutz.ch