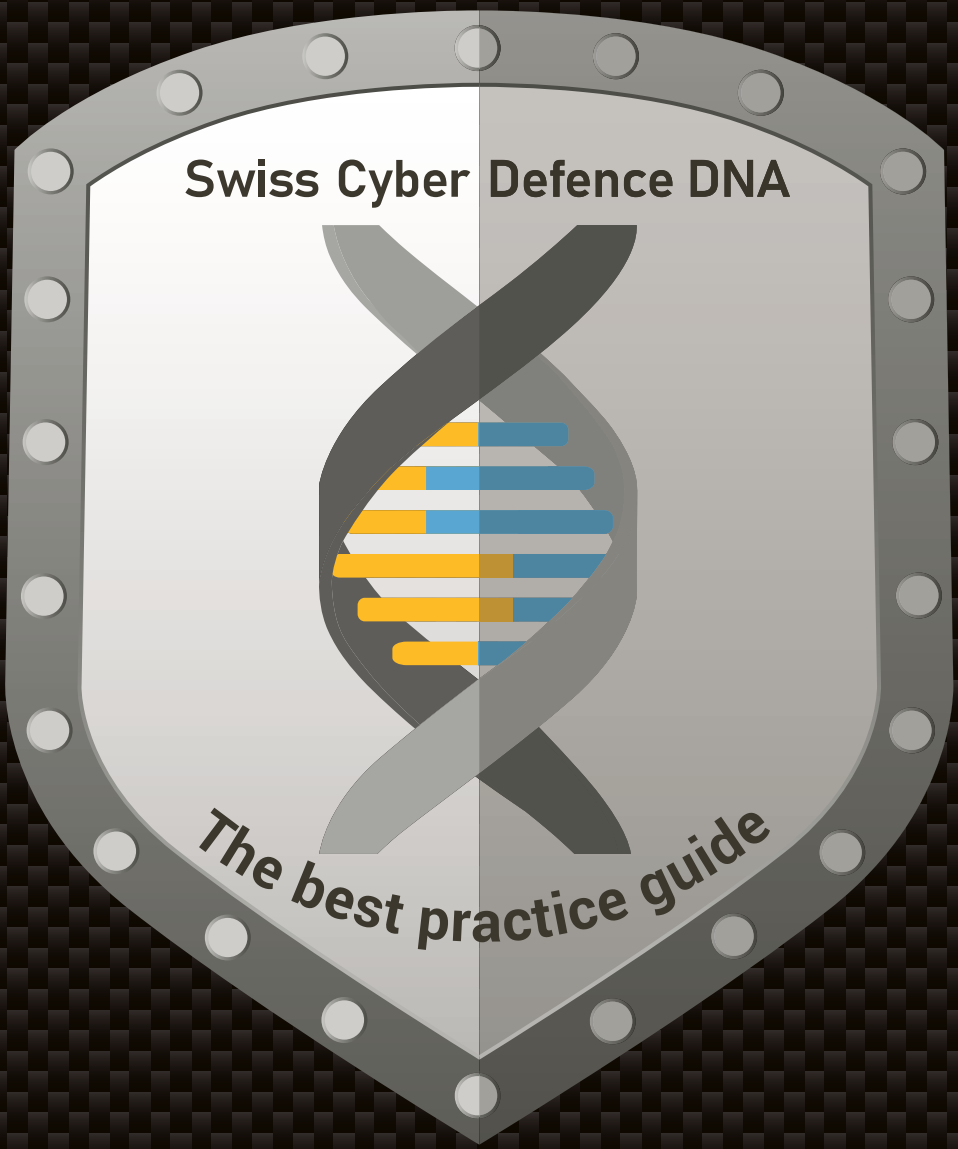
Protection against blackmailing for SMEs



The essence for your survival in the digital age

Swiss Cyber Defence DNA

The main things you need to do to survive in the digital age

Swiss Cyber Defence DNA (SCD-DNA) is a guide for your SME, designed to help you protect yourself easily and efficiently against the dangers of cybercrime and major financial losses. Set the hurdle for cybercriminals so high that you cannot be blackmailed. SCD-DNA is an initiative of MOUNT10 AG with the participation of various industrial partners.

The following catalogue of measures takes the organisational and technological responsibilities within your company into account.

Measure No. 1 – Up-to-date unchangeable data backup/write-protected backup

Secures the survival of your company, in the same way as an airbag in a car

- ☐ Define a person for implementation and review
- ☐ Ensure external storage of the backup
- ☐ Automated, write-protected backup process including encryption
- ☐ If the above is not possible: disconnect the backup medium from the network and store it offline

Measure No. 2 – Comprehensive and up-to-date protection against malware

This is your first line of defence, like a safe front door

- ☐ Awareness-raising and training of employees with regard to dealing with e-mails, websites, passwords etc.
- ☐ Comprehensive, companywide malware protection for end devices, servers, cloud and e-mail services
- ☐ Restrict macro execution; Install internet and spam filter

Measure No. 3 – Harden networks and remote access

Your defences for selectively preventing unauthorised access

- ☐ Training of employees and suppliers for remote access
- ☐ Use a firewall to divide your network into zones so that important business areas are segregated
- ☐ Additionally secure remote access using 2-factor authentication (e.g. SMS code)

Measure No. 4 – Keep hardware and software up to date

Your guarantee for a secure, properly functioning IT

- ☐ Define a person who is responsible for the administration and periodic review of the licenses/updates
- ☐ According the risk assessment, replace outdated systems and physically protect existing ones (e.g. access to the server)
- ☐ Use only current operating systems and applications
- ☐ Isolate old systems from the network

Measure No. 5 – Employees and their roles

Your self-protection with limitations to what is strictly necessary

- ☐ Use a role concept to define which rights are necessary for each employee
- ☐ Also check and restrict management access rights
- ☐ Create password rules for employees
- ☐ Link and restrict defined roles with the access rights

Measure No. 6 – Define emergency processes

Your protection in an emergency by means of a clearly defined plan instead of improvisation

- ☐ Determine the emergency organisation, define processes and inform all employees
- ☐ Regularly review roles and processes and restore data frequently
- ☐ Use independent technology to ensure documents can be accessed even in an emergency (e.g. emergency note, paper folder, cloud or mobile solution)

You can find more information at scd-dna.ch

Sponsorship

TREND MICRO

MOUNT10
SWISS DATA DEFENCE

Hewlett Packard Enterprise

COMPASS SECURITY

SOPHOS
Cybersecurity evolved.

atrete
IT consultants

swisscom

Microsoft

CISCO

SWISS POST

helvetia

Patrons, Contributors & Web partner

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

Presented by

More information at
kmuschutz.ch