RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

DEFENCE-IN-DEPTH: A METHODOLOGY

The concept of defence-in-depth is based on the principle that any security component or measure can be bypassed. It relies on a **coordinated combination** of technical, organisational, and physical measures aligned with **attack scenarios**, in order to increase the effort and resources required for attackers to achieve their ends, to facilitate detection, and to limit the operational impact of attacks. This approach is defined by the use of **multiple robust** and **independent** security layers, designed to ensure that no single attack can bypass several safeguards simultaneously.

The implementation of this strategy must be iterative and prioritised according to risks, relying on the four pillars of **governance**, **protection**, **defence**, and **resilience**.

1/ GOVERNANCE – MANAGEMENT AND SCOPE

Governance aims to frame and pilot digital risks using organisational measures to anticipate threats, maintain security levels, and continuously strengthen the security of information systems (ISs).

- **Establish a risk management strategy** to identify and prioritise risks, notably by establishing an IS mapping, performing and maintaining a cybersecurity risk analysis (e.g., EBIOS RM).
- **Identify and regularly audit** stakeholders in the ecosystem to control risks throughout the supply chain. These measures may be imposed on subcontractors, for example, to ensure the protection of the entity's sensitive data or the security of developments.
- **Conduct regular audits on the security measures applied to the entity's ISs**, before commissioning and throughout their entire lifecycle.
- **Raise awareness and train users and external stakeholders** on security within their areas of responsibility.
- **Continuously monitor vulnerabilities and threats** affecting the IS.

2/ PROTECTION – PREVENTING AND BLOCKING

Protection measures are intended to prevent or block attacks on the IS by reducing the attack surface and making any attempt to target the entity's primary assets more costly.

- **Protect physical access to the IS** to prevent unauthorised access to critical components, for example through physical access control mechanisms and video surveillance (guide only available in French).
- **Segment and filter communications** to reduce the attack surface, limit lateral movement, and apply differentiated security policies by security zone, paying particular attention to administrative networks.
- **Control logical access to the IS** to ensure the traceability of actions, and apply the **principle of least privilege**, notably by strengthening authentication mechanisms, securing directories, and limiting credential exposure (guides only available in French).
- **Protect data at rest and in transit** to ensure confidentiality and/or integrity. Cryptographic mechanisms (guide only available in French) should be used according to their exposure and criticality.
- **Maintain the IS in operational and security condition (MCO/MCS)** to ensure its robustness throughout its lifecycle by implementing patches or specific compensatory measures according to the entity's specific risks.

V1.0 (07/26)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

3/ DEFENCE – DETECTING AND RESPONDING

Defence measures enable a proactive posture to detect and respond to malicious activities, thereby reducing the impact of an attack on the IS.

- **Define a threat detection strategy** to detect relevant attack scenarios, articulated around: (i) **collecting** IS events and (ii) real-time **detection** of suspicious activities by creating and maintaining correlation rules.
- **Define an incident response strategy** to regain control of the IS: alert qualification, attack containment, evidence collection, and eradication of residual footholds.

4/ RESILLIENCE – RESISTING AND RESTORING

Resilience measures aim to resist attacks and restore the IS to a normal state of operations, ensuring continuity of activity with an acceptable level of degradation, through a progressive recovery process limiting business impacts.

- **Define a business continuity and disaster recovery plan** (BCP/DRP) to maintain services in a degraded mode (resources or infrastructure backup, backup site, etc.) and restore the system to a normal state of operations, including through backup and restoration procedures.
- **Define a crisis management plan** to ensure strategic decision-making, team coordination, and crisis communication (guides only available in French).
- **Assess, on a regular basis, the resilience of the system** and the organisation through crisis management exercises, as well as BCP and DRP tests.

5/ IMPLEMENTATION PROCESS

The implementation of a defence-in-depth strategy for a new or existing information system must be tailored to the system's criticality and degree of exposure to threats. An iterative approach is recommended.

- **Establish a system reference baseline** by identifying its scope, ecosystem, critical assets, their interdependencies, as well as the applicable security measures and their current implementation status.
- **Define security objectives and targets**, in line with the criticality of the information system's missions and exposure to threats.
- **Ensure the multiplicity and variety of measures** by combining protection, defence, and resilience in light of threat scenarios.
- **Ensure the robustness of security measures** through regular assessments, the use of trusted building blocks, and the deployment of updates.
- **Ensure threat detection of ISs** once they have reached a sufficient level of maturity in terms of protection, in order to identify any potential circumvention.
- **Prioritise the independence of measures** to prevent a single attack method from bypassing several security measures. This includes, for example, technological diversity in the solutions deployed or avoiding hosting multiple security measures on the same physical platform.
- **Ensure continuous improvement** by regularly assessing the organisation's security posture and adjusting measures, in line with feedback and state-of-the-art information security practices, based on changes in the threat landscape.
- **Prioritise strengthening the pillars of governance and resilience** before improving protection and defence measures. Above all, it is essential to ensure that the information system is fully under control, and that the organisation is capable, in the event of an incident, of rapidly switching to a mode which, although degraded, allows core activities to remain operational.
- **Strengthen protection and defence measures**, in line with organisational capabilities, to ensure their robustness over time. An organisation that is mature across all four pillars can then deploy advanced mechanisms, dynamically combining protection and defence (Zero Trust model).

V1.0 (07/26)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr