RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

DEFENCE-IN-DEPTH: IMPLEMENTATION

The implementation of defence-in-depth requires the introduction of **complementary security barriers**, each of which is made up of a set of **measure**

This approach defines a barrier as a security objective responding to a stage in a risk scenario, whilst a measure constitutes the basic unit (organisational, technical or operational): its function contributes to the attainment of a barrier's security objective." ?

The implementation of a barrier hinges on three key pillars:

- **its role (the "what")** in addressing a risk scenario: protection (before), defence (during), and resilience (after);
- **its location (the "where")**, applied to the components of an information system: user, premises, identity, network, equipment, application, and data;
- **its implementation (the "how")**, according to the security measures chosen to meet its security objective.

The overall effectiveness of this strategy relies on three criteria – **multiplicity, independence, and robustness** – applicable at the level of:

- **barriers**, to ensure that the information system has successive and autonomous defences capable of countering each stage of an attacker's progress;
- **measures**, to ensure that each barrier is itself robust and relies on varied, complementary measures, as well as on distinct technological foundations that do not share the same weaknesses.

The independence of the various security barriers (protection, defence, and resilience) is a particularly important criterion. The failure of a protection barrier within the production information system should not result in a loss of visibility from the monitoring information system, nor should it compromise the resilience barriers of the administration information system.

The implementation of security measures on an information system must be tailored to its level of exposure, its criticality, and the identified risk scenarios. The following example addresses only one possible risk scenario amongst various others which could enable an attacker to achieve their objective; it is therefore not exhaustive. It must be adapted to the specific context of an information system, and supplemented by other measures to cover all scenarios.

1/ IMPLEMENTATION EXAMPLE

To protect against a ransomware attack, the following defences and measures could be deployed:

- **Detect and block phishing attempts (defence, network):**
  - keep detection rules up to date;
  - analyse emails statically using signatures and dynamically in a sandbox;
  - use an inbound gateway to carry out these analyses upstream of the email server.

- **Minimise the likelihood of a user executing malware (protection, user):**
  - raise awareness regularly about phishing attempts;
  - test user behaviour through internal phishing campaigns.
- **Limit an attacker's ability to install tools (protection, equipment):**
  - restrict user rights on their workstations in accordance with the principle of least privilege (e.g. do not grant administrative rights);
  - ensure that security patches on workstations are up to date.
- **Detect and block the installation of malwares (defence, equipment):**
  - carry out behavioural analysis on user workstations (e.g. EDR);
  - ensure that detection rules on workstations are kept up to date.
- **Limit an attacker's ability to establish a command-and-control channel to the Internet (protection, network):**
  - implement a proxy server for Internet access and a DNS resolver for public domain names in the DMZ; ensure these cannot be bypassed by default;
  - keep filtering rules up to date.
- **Limit an attacker's ability to lateralize by compromising a privileged account on a workstation (protection, identity):**
  - use dedicated administrator accounts on user workstations;
  - carry out regular audits of the central directory service.
- **Mitigate data loss (resilience, data):**
  - implement a data backup mechanism with at least one offline copy;
  - regularly test backup and restore procedures.

2/ EXAMPLE OF BARRIERS

Generic barriers	Applicable component	Example of measures multiplicity	Examples of measures independence	Examples of measures robustness
Protection: User authentication	Identity	Multi factor authentication	Use of a physical token separate from the system access terminal	Cryptographic challenge-response authentication Appropriate sizing of secrets
Defence : Anomaly-based flow analysis	Network	Multiplicity of points for collecting and analysing data flows	Centralisation of alerts on dedicated servers separate from the production environment Position the sensors behind physical TAPs	Keeping detection rules up to date Improving the reliability of alerts
Resilience: Cold standby site	All	Redundancy of critical functions necessary for business continuity	Complete independence of the fallback components from those used in production.	Regular testing of fallback procedures Maintenance in operational condition for fallback components