Enhancing the effectiveness of secure by design through the integration of business continuity management (BCM)

August 2024

Christian Müller

According to the German Federal Office for Information Security (BSI), the cyber security risk posed to businesses is at an unprecedented height. While a minor fraction of cyber security breaches can be attributed to newly discovered vulnerabilities (zero-day), most stem from vulnerabilities or attack methods that have already been discovered, documented and published (known exploits) and other weaknesses that could have been detected during system implementation. If these risks, which are either unidentified or insufficiently addressed, infiltrate critical processes, a small security incident can rapidly escalate into a dire emergency that poses a significant threat to the company.

Ensuring cyber security through secure by design

Identifying risks associated with cyber security threats is a fundamental aspect of information security, which is part of the secure-by-design-process. Various methods, notably security baseline, security risk assessments and thread modelling, are frequently used for risk identification and preventive measures.

The application of these secure-by-design methods are employed with the objective of maintaining an adequate level of security during the execution of projects and changes. The challenge lies in harmonising the effort required for the comprehensive implementation of these methods with the constrained resources available, both technically and in terms of security. Providing maximum protection across all areas would not be economically viable or efficient, even if resources were unlimited.

The central question is how a company and its security department can ensure the utilisation of appropriate methods to identify, assess, and manage risks effectively, and despite resource limitations.

The security-baseline method defines the minimum requirements for systems; relying solely on it, although it saves on resources, is not a viable strategy. This is primarily because risks – particularly in relation to their existence, likelihood and impacts – often cannot be adequately identified, evaluated or managed due to insufficient information. While the application of security baselines can generally achieve a security level deemed appropriate for the majority of systems, considering additional technical or organisational measures, it may be inadequate for critical systems.

Therefore, companies must determine when security baselines are sufficient, and when more in-depth analyses and examinations are required for risk assessments, such as scenario-based risk analyses or even thread modelling, to fully evaluate risks that demand a correspondingly higher effort.

The criticality assessment of the protection objectives for information security (confidentiality, availability, and integrity) provides an initial approach to evaluating the need for protection. However, this approach is limited as it only partially considers the technical aspect. An alternative approach would be to evaluate the criticality for the company if a disruption occurs (due to an unidentified risk after implementation) to the implemented system, process or associated systems or processes.

By combining the need for protection from an information-security perspective and the criticality of a potential failure, the company can prioritise the level of effort and thus determine which methods are most appropriate.

Optimising secure by design through BCM

BCM is key in addressing this challenge. Its primary objective is to pinpoint critical business operations, safeguard them, and thereby guarantee the company's uninterrupted functioning. In this scenario, BCM employs a notion of 'criticality' that is not typically found in information security. It defines processes as critical if they would, if disrupted, pose a substantial risk to the value-creation process.

By using the 'criticality' concept from BCM, the secure-by-design process can better establish priorities, enabling a more strategic allocation of resources. To achieve this, it is meaningful to incorporate suitable BCM strategies into the secure-by-design process. This integration ensures a more robust and resilient system, capable of maintaining business continuity even when faced with unforeseen disruptions.

- **Pre-filtering**: During the planning of a project or change, systems are assessed according to their involvement in processes critical to value creation in addition to how critical its assets are against the objectives of information security (confidentiality, integrity and availability).
- **Business impact analysis**: This analysis evaluates whether a failure of the component, either directly or indirectly via dependencies (or the failure of dependent components) would have a time-critical impact on the process, or if there is a high criticality according to information security objectives. For the use of the concept in the secure-by-design process, a rough evaluation could initially be carried out at the process level during the business impact analysis. The otherwise usual evaluation at resource level could be carried out subsequently if the criticality is appropriate.

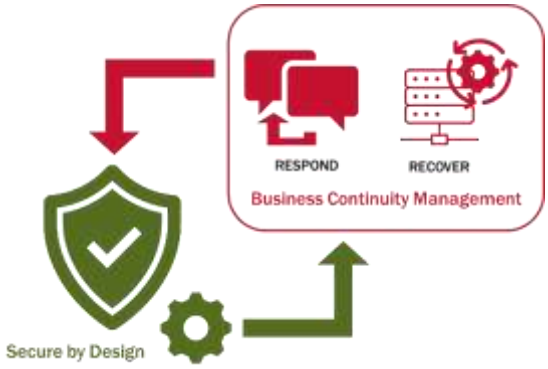
If both pre-filtering and the business impact analysis indicate a corresponding high criticality to information security or business continuity objectives, then the implementation or change, along with the affected components and other resources, would be prioritised in a secure-by-design process. This process involves the evaluation of risk scenarios and threat modelling, supplemented with results from business impact analysis and risk assessments.

This allows for a comprehensive evaluation of threats, vulnerabilities, impact, and probability, and enables the planning of responses to potential emergencies in advance.

The security of non-critical implementations and changes could be evaluated in a more resource-efficient manner via security baselines and, if necessary, risk assessments.

While the integration of business continuity management into the secure-by-design process will not influence the global threat landscape, it can significantly reduce the impact on companies.

Figure 1: BCM and secure by design interaction



Source: Analysys Mason

How can Analysys Mason support your business?

Ensuring cyber resilience is not only a legal necessity in the face of a high-threat situation, but also a compelling challenge for companies to effectively respond to threats, particularly from cyber-attacks. At Analysys Mason, we firmly believe that security and business are not adversaries, but collaborators acting in the company’s best interest. We are committed to providing targeted support to you and your company. Leveraging our extensive track record in business-process and cyber-security transformation, we can help you to navigate this complex journey and pinpoint the right measures while simultaneously ensuring security and compliance. Our approach begins with analysing the specific regulatory and internal requirements of your company and the business processes within your company. We then develop and implement a comprehensive strategy and process to bolster resilience in anticipation of future security incidents. As the capabilities of cyber criminals continue to escalate, we ensure that your company is equipped to tackle the upcoming challenges.