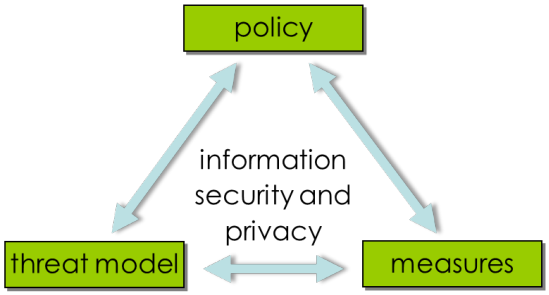
Still clinging on to the illusion that your data is safe and sound? It's time for the red pill!

Cyber Security, Information Security and Privacy

Overview

Cyber security and information security focus on the protection of information and data in organizations, business processes, and information systems from undesired use or manipulation. The needs of customers, employees, and partners play a crucial role for a sound security policy. Privacy focuses on the compliant use of information and data about individuals and corporations.
Many of today's modern products and services rely heavily on internet-connected information systems and data during their entire life cycles. With the Internet of Things (IoT) this trend will surely continue. Products and services are ever more exposed to threats regarding e.g. the availability of critical systems and data integrity.
A structured threat model, a clear security policy and adequate measures to deal with security threats, is key to safe and sound data. This ensures achieving reliable, uninterrupted business services to the benefit of customers, employees as well as partners.



Policy – information security and privacy goals including an implementation strategy. Classic categories for these goals are confidentiality, integrity and availability.
Threat model – a model about known threats, assumed threats and assumptions about adversaries. This model includes risk assessments that consider expected probabilities of threats and the severity of their consequences.
Measures – elaborated measures to adequately counter relevant risks identified in the threat model. Depending on the context, measures can include: implementations in software, hardware and systems; rules, guidelines and training for employees; business process and organizational changes.

KnowGravity Inc. offers **security engineering as a service** tailored to your needs – for organizations, teams, projects, business- and development processes as well as products and services.

Security engineering for organizations

- Implementation of structured and adequate information security management systems (ISMS) in an organization, a department or information security team. Guided by ISO27000 standards family or BSI IT-GS (BSI Standard 100-2), tailored to your needs.

This service typically includes at least the first four points of the following listed activities.

Security engineering for organizations, projects, processes and products

This service typically includes one or more of the following activities:

- Brief analysis and description of the organization/project/process/product, particularly its goals, structure, management approach, environment and context regarding security management, definition of scope.
- Adaption/definition of an **information security policy** with security goals and implementation strategy in collaboration with stakeholders.
- Adaption/definition of a **threat model**, elicitation and analysis of known and assumed security threats, their risks and possible causes with stakeholders.
- Adaption/definition/implementation of **adequate measures** with stakeholders to counter threats and lower identified risks (threat model) to ultimately achieve security goals and enforce the security policy.
- Adaption/definition/implementation of **assurance and continues improvement** processes for security management.
- **Assessment** of implemented measures, threat models and policies.
- Organization of interviews/workshops with organization/project/product team members and stakeholders to e.g. identify and document the state of information security management, elicit security and privacy threats, risks and causes, elaborate security goals, define adequate measures, elaborate security processes.
- In depth **analysis of potential security threats** and risks as well as weaknesses of a subject, e.g. an application, a development process, a team in an organization.
- In depth **analysis of potential data privacy threats**, risks, weaknesses as well as data privacy **compliancy** for an organization/a process/a project/a product.
- Production and presentation of security policy, threat models, compliancy reports and security measure documentation for stakeholders, employee training.

Related Services

- In addition to security and privacy requirements, KnowGravity may further elaborate functional and non-functional requirements by applying Model-based Requirements Engineering (MBRE).
- Model-based Risk Analysis (MBRA) may further help analyze and manage risks in a structured way by supporting the identification of sources and causes of risks, the estimation and quantification of consequences and elaboration of suitable measures.

Why KnowGravity?

- KnowGravity is familiar with information security-related standards such as ISO27x, BSI IT-GS (BSI Standard 100-2) for organizations to OWASP for web applications.
- Employees of KnowGravity combine years of experience in the security domain: elaborating and implementing ISMS in big organizations; securing project processes; analyzing organizations, business processes, systems, applications for security, privacy and compliance issues; requirements engineering for security applications (e.g. IAM).
- KnowGravity has comprehensive engineering experience in a wide spectrum of domains and techniques, including mission- and safety-critical systems.
- KnowGravity is an active OMG member in the testing and risk analysis domain as well as in several other modeling working groups and supports OMG's SEMAT/ESSENCE approach for agile project management.
- All employees of KnowGravity are modeling experts for business systems as well as for technical systems and are proficient in many domain specific modeling languages.
- Employees of KnowGravity are co-authors of a book on operational risks.

Contact

KnowGravity Inc.
Hohlstrasse 534
CH-8048 Zürich

Phone +41 44 43 42 000
Internet www.knowgravity.com
E-Mail info@knowgravity.com