WEB 2.0 SERVICES SECURITY: MATRIX AND VIRGILIO.IT

Matrix S.p.A., a company of the Telecom Italia Group specialized in the creation of Web 2.0 services and in marketing on web and mobile channels, developed and implemented, in cooperation with Spike Reply, an innovative management process of all aspects concerning the functional and technology security of its products. An important part of the activity consists in raising awareness, among employees and co-operators having business-generating tasks, so that security is no longer seen as an obstacle to Time To Market, but rather as an opportunity.

CONTEXT

Matrix S.p.A. is a historic company within the Italian internet scenario. It offers users innovative Web 2.0 services

Within the Telecom Italia Group, Matrix S.p.A.:

- Manages the creation of Web 2.0 services on internet and mobile channels
- Manages web and mobile marketing initiatives through the advertising agency Niumidia Advertising
- Plans, develops and delivers VIRGILIO.IT services to millions of users, including electronic mail, social networking and portal information services

WEB 2.0 SERVICES SECURITY NEEDS. At Matrix, like within all the production cycles of any IT company, regulatory requirements, business quality, reliability and strength over competitors are key elements for the success of a product or of a service. For web applications, the attention paid to all these production aspects is not enough, unless equal attention is paid to the security aspects. This issue is extremely important, though made more complex by the new Web 2.0 *Business Models.* In virtue of these changes, both the security threats to which the services offered by web applications are exposed, and our customers, have changed. In order to face such new threats it is necessary to set up an integrated security process and identify methodologies and technologies able to ensure the security of a web product or service.

AWARENESS ON SECURITY ISSUES. Companies whose business is linked to security, in a way which is not always so apparent, need to be made aware of security issues, in order to better understand which aspects may represent a constraint and which aspects, on the other hand, may be useful and generate opportunities.

WEB MISUSE. Virgilio, like all social network providers, is subject to different kinds of misuses, from Cyberbullying, to the publishing of illegal material (for ex. pedopornography, copyright, etc). All such measures top up with other possible types of violations to the detriment of users like password violation, Identity theft or denial of service.

SOLUTION

Within Matrix S.p.A., the management of web services security requires the competences of all business functions: people in charge of security management provide the specific skills, people in charge of development provide process knowledge, marketing specialists provide the knowledge on the impacts on customers and on business. Together, they all cooperate, with their own specific skills, in order to coordinate and create products which may be considered safe.

DEFINITION OF A MANAGEMENT MODEL FOR WEB 2.0 SECURITY. Further to numerous activities carried out with customers, we have innovated security management by creating, in tight cooperation with the Client, a new model of security control taking into consideration all the real and special security requirements of Companies operating in the Web 2.0 world.

THE SECURITY AWARENESS PROGRAMME. Training and sensitizing Business personnel is of strategic importance, since it provides the cultural tools to understand the business opportunities that may be seized by tackling the Web 2.0 product security issues in a structured way. The delivery modalities of the awareness program consist in: courses focusing on specific issues linked to the Matrix business, production and dissemination of information material and delivery of a press review on the most important security events found on the most authoritative web sites, together with business contextualization information by the Security function.

THE INTEGRATED PROCESS FOR THE SECURITY OF WEB PRODUCTS. The Company shall be able to ensure the security levels of the Web 2.0 services it offers, as required by the regulatory constraints, by the Company's security policies and by the service users.

Therefore, the security function, becomes the competence and service center for all functions responsible to create web applications, thus governing a non-intrusive process towards the Company, aimed at measuring the real residual risk of a provided service.

Parallel to the project **design** phase, the security process supports the activities highlighting possible requirements and constraints and the analysis of the security functionalities that the product or service wish to offer. The integration between the security function and the people in charge of the product design is a strategic integration, since such people may not have the necessary skills to consider all legal requirements or known problems relating to the security of the product or service that is being developed.

The initial phase, during which requirements are defined, is also an opportunity to develop products and services having an added element, compared to competitors who do not consider security issues as real Business opportunities. Cooperating with the security function in the initial phase, allows to carefully and accurately plan the work and sets the basis for the creation of a strong and durable product or service.

The product "risk classification" is made jointly with a **feasibility** study concerning the service, and allows to measure the resources to be allocated to a specific product or services, on the basis of its criticity. Through the use of methodologies geared towards the analysis of web threats and vulnerabilities, the security function calculates, documents and communicates, to the people in charge of business, the real company exposure to the risk.

The Security function adopts specific security-oriented methodologies, best practices and tools during the **development phase,** since this represent the only way in order to remedy application vulnerabilities which allow intruders to commit violations and jeopardize the business. During this phase, the security function represents the service center at the disposal of the Development Team. Particular attention is paid to the **testing** phase, which is specifically "targeted" and does not merely concern the functional characteristics of the application. As a matter of fact, this phase tests the real compliance of the web application to the guidelines of safe programming. The application Penetration Testing activities are a fundamental tool for this type of activities as they complement the code analysis performed during the development phase.

REPLY VALUE

Spike Reply was able to understand the real customer needs, analyze the cultural and organization context and set up a strategy for the creation of a Security function which could be considered both competent and effective.

Reply's methodology proposal was recognized as innovative, thanks to the Business levers used to create a security culture within the Company.

Within the Reply SpA Group, Spike Reply is the company specialized in the field of Security and Personal Data Protection.

Spike Reply developed a comprehensive, integrated and consistent offer, in order to tackle any aspect of risks associated to an information system: from detection of threats and vulnerabilities to the definition, planning and implementation of technology, legal, organization, insurance or risk retention counter-measures.

Spike Reply
www.reply.eu