Application Security Report

Application Security Report is an annual SYNTAX publication summarizing the vulnerabilities discovered on application security engagements and provides an insight on current web and mobile application vulnerabilities.

Syntax IT Inc.

216 Mesogeion Avenue.
Holargos 155 61
Attica, Greece

Tel.:+30 210 65 43 100

sysec@syntax.gr

10/14/2013

CONTENTS

BRIEF PROFILE

SYNTAX IT Inc. was founded in 1994 as the business evolution of ArAmIS Inc., the groundbreaking IT consulting company for large corporations all over the Arabian Gulf. The company is based in Athens, Greece, and is active across Europe and the Arabian Gulf. With the association of SYNTAX Diamond IS LLC, a member of the Royal Diamond group of Abu Dhabi UAE, operates in EMEA and has formed the SYNTAX IT Group in 2011.

SYNTAX collaborates with some of the largest and most innovative global high technology corporations, as well as with cutting edge academic and research institutions in Greece and throughout Europe. Some of the most significant organizations from the Financial, Telecom, Energy, Transportations and the greater Public Sector feature prominently in SYNTAX's client roster.

SYNTAX Ethical Hacking team was formed at 2008 delivering high quality services on the EMEA region. It has conducted numerous penetration tests, vulnerability assessments and source code reviews on a variety of environments such as internal and external networks, web applications and mobile applications.

SYNTAX consultants are also trained in high level security technologies, such as Endpoint Protection, Data Loss Prevention, Encryption, Compliance Management, Business Continuity, Identity Management, as a consequence of the numerous and prosperous partnerships with Symantec, WhiteHat, CA, Skybox, etc., giving them a more holistic approach in the area of Information Security. Therefore, they are trained into implementing security services and new protection technologies; those they have to bypass when they are engaged into penetration tests and vulnerability assessments. This helps our consultants stay up-to-date with the cutting edge technologies and on the same time, provide our customers services giving added value on the whole field of Information Security.

SYNTAX METHODOLOGY

The methodology that SYNTAX has developed for its ethical hacking services demonstrates some significant advantages compared to other methodologies. These advantages are not only a result of the advanced techniques that are used for the analysis of the vulnerabilities but also from the overall management and the expertise of the team that undertakes such projects.

SYNTAX has developed its methodology based on established international standards, methodologies and best practices such as: OSSTIMM, OWASP Testing Guide, OWASP ASVS, NIST SP800-115, NIST 800-30. It is a repeatable procedure, offering our security consultants the ability to compare results and assess different environments more accurately.

Moreover, SYNTAX methodology is being constantly updated and kept up-to-date. As new vulnerabilities and exploitation methods emerge, the internal methodology has to keep that pace.

SYNTAX offers a state of the art deliverable (report), which offers multiple advantages to its clients and adds real value to the relative penetration testing services. The report is an aggregated and very comprehensive “snapshot” service deliverable, which offers from a high-level summary of findings to a very detailed explanation of the vulnerabilities identified. Very explanatory remediation steps are also included on the deliverable, which allows clients to start remediating vulnerabilities from day 0.

Last but not least, SYNTAX security consultants enjoy the privileges that offer many personal and corporate partnerships. Regarding OWASP membership, consultants take part in the big application security community, share their experiences and knowledge and gain a lot of expertise and know-how, needed for the challenging day to day penetration tests and vulnerability assessments.

EXECUTIVE SUMMARY

SYNTAX Application Security Annual report aims at developing and raising the security awareness regarding application vulnerabilities. The present, first publication, was created with a view of contributing and offering the expertise and knowledge to the global application security community.

This annual report summarizes the application security posture of the web and mobile applications tested in the last two years. This data is from a sample of penetration tests carried out on 2011 and 2012 on the EMEA region. It was processed and presented accordingly, in order to protect our clients and on the same time, reach useful conclusions regarding the posture and the trends of application vulnerabilities. It comes from a variety of web applications (internal, Internet exposed) and range of organizations.

In a high-level the report can be summarized on the following points:

- From the web applications tested, 1 out of 4 (**24.77%**) suffer from **Platform Security Misconfiguration**.
- A very large portion of vulnerabilities identified (**16.21%**) affect **Data Validation and Encoding** issues.
- Equally number of vulnerabilities affects the **Communications' Security** (**14.98%**) and the **Session Management** (**14.68%**) of the web applications.
- The majority of vulnerabilities identified in mobile applications affect the handling and storage of the data (**37.50%**).
- The dominant section of source code vulnerabilities affect the **Input Validation** (**25.78%**).

In a nutshell, the applications (web and mobile) suffer from vulnerabilities that affect the **Data Validation** (data input and output), the **Session Management** and the **Communications Security**. As a consequence, the attack vector against the web applications is large and multi-level. The dominant vulnerabilities promote attacks against the web application thought the data exchanged, the user's session and the network communication layer.

Distribution by Industry

Figure 1 shows the distribution of the applications by industry.

The majority of the applications are owned by Financial Institutions (Banking). Those organizations are under the scope of strict mandates and compliance requirements (e.g. PCI/DSS) and they are enforcing application security thought-out the software development lifecycle. Moreover, they are often targeted by organized crime and therefore, the need for an integration of a secure code development lifecycle to their procedures, is imperative.

The second dominant category is the Government applications. This is mainly due to the fact that governmental websites and portals are not only under the scope of the organized crime but also under the scope of well-known, renowned "hactivist" groups. Those applications may disclose sensitive information of individuals, if they are successfully compromised.

The rest of the applications are distributed equally between the Aerospace & Defence, Software/IT services and Telecommunications. All of the above industries, are looking in securing either the applications they are using (internal or Internet-facing) or the applications they are developing and selling to their end customers.

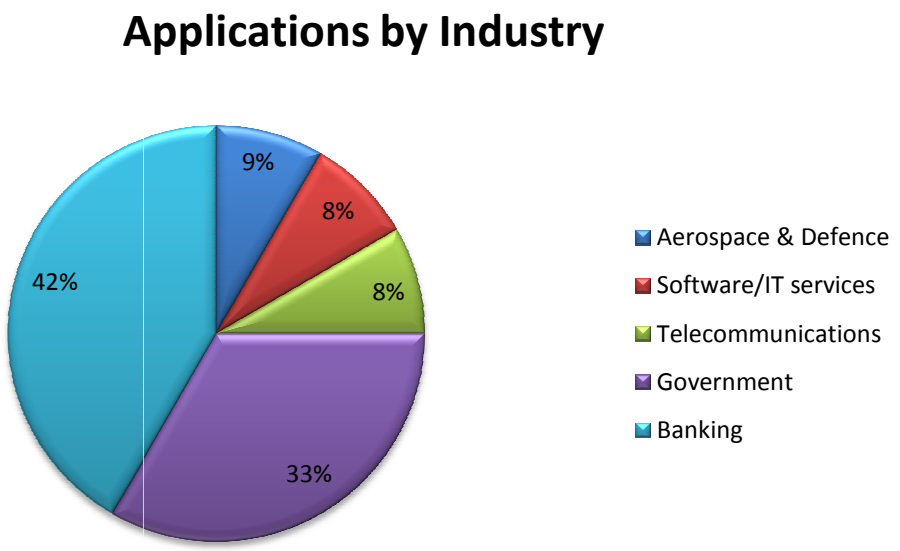

Figure 1: Applications by Industry

Business Drivers for Risk Mitigation

Figure 2 illustrates the business drivers for running the penetration tests and vulnerability assessments, and generally the reasons for mitigating the vulnerabilities identified.

The majority of the customers are driven by compliance and regulatory requirements. Penetration tests and vulnerability assessments are, on the most cases, part of information security programs and a form for key business people to prove due diligence. Even though compliance actually sets a security baseline among organizations, it does not necessarily integrate security best practices on the software development lifecycle. Application security is being evaluated more as a checklist procedure than a business strategy that adds a competitive advantage to the organization.

The second business driver is the Information Security Policy of the organization, which anticipates vulnerabilities' identification and mitigation (or acceptance). The next business driver is Risk Reduction. Actually, it is a category of a driver where there is neither regulatory requirement nor information security policy that demands vulnerabilities' remediation; organizations act on their own self-motivation in order to identify and mitigate the risks. Second last is the customer demand, where the organization wants to produce and sell software tested against the industry current best practices.

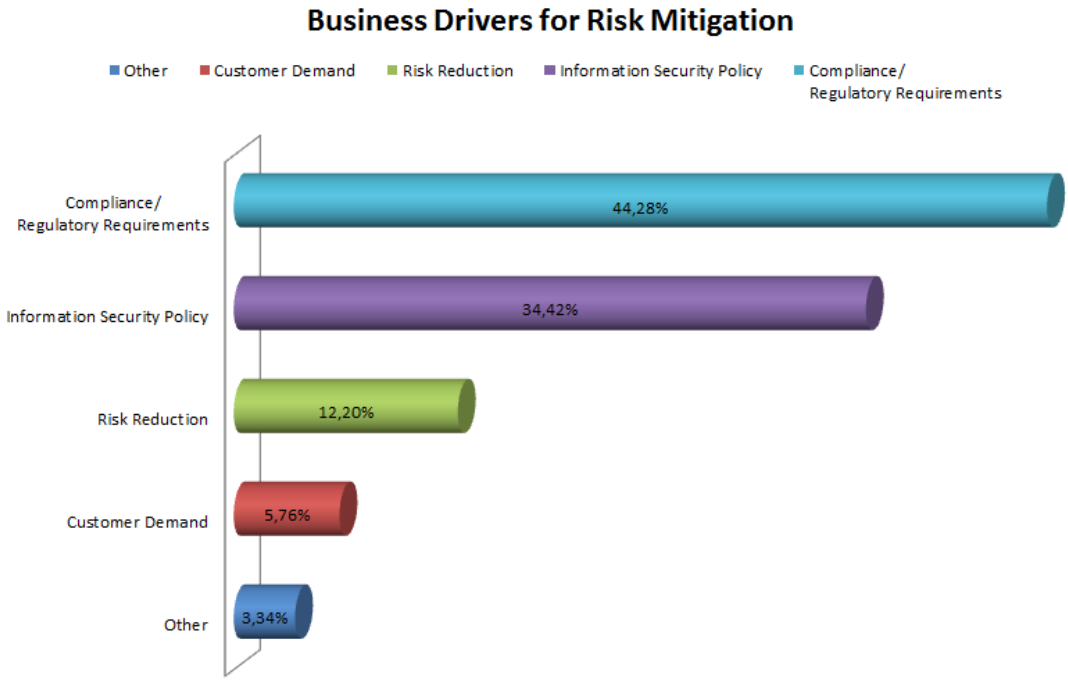

Figure 2: Drivers for Risk Mitigation

Risk and Impact Breakdown by Severity

Web Applications

In the following graphs, business impact and overall risk is being categorized by severity.

Business impact is comprised of a variety of factors. Indicative, those include the financial and reputation damage, non-compliance, privacy violation issues, disruption of business activity (and business continuity) and reduction in operational efficiency/performance that a vulnerability may cause, if it is successfully exploited by an attacker.

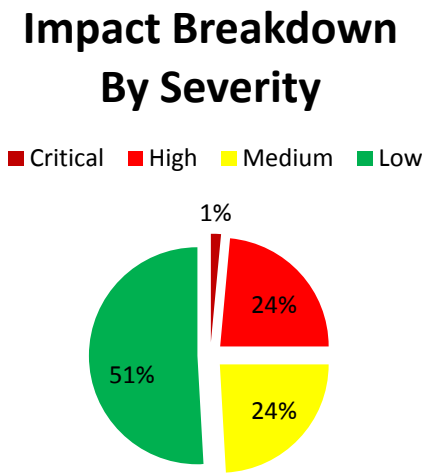

Figure 4: Business Impact Breakdown by Severity

way than the internal procedures.

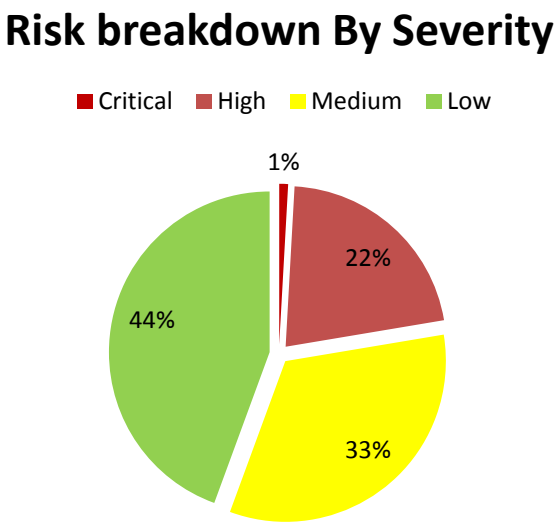

Figure 3: Risk Breakdown by Severity

Overall risk is calculated by following the most important risk management and assessment models. The main steps in evaluating the risk are: the threat and vulnerability identification, likelihood determination and business impact analysis. All these metrics are integrated determining the overall risk of the vulnerabilities being identified.

The categorization of the risk may vary between our consultants and the clients. Outsource consultants follow methodologies which often evaluate the risk in a different

Mobile Applications

Mobile applications findings give a different distribution of risk and business impact. This is rational up to a certain point because of the immaturity on the area of developing mobile applications following secure code application development techniques and standards. **62.50%** of the vulnerabilities discovered posed a **high risk** to the organization, whereas the **12.50%** were **medium** risk issues and the **25%** were **low** risk issues. This figure (figure 5) depicts the risk an organization can face due to vulnerabilities of a mobile application.

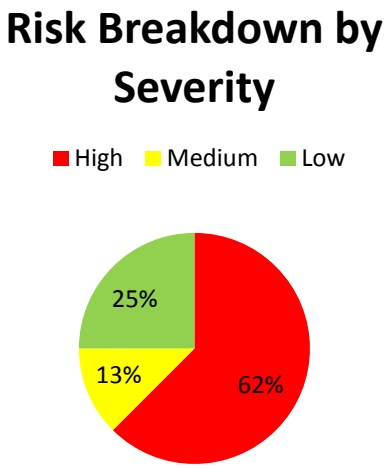

Figure 5: Risk Breakdown by Severity

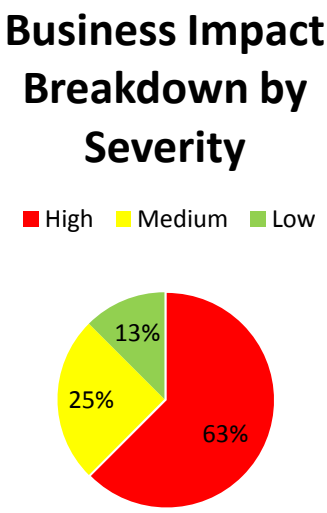

Figure 6: Business Impact Breakdown by Severity

Concerning the business impact of the vulnerabilities identified, high impact vulnerabilities rate remain **high: 62.50%**. On the following categories we have a difference with overall risk; **25%** of the vulnerabilities were ranked of a **medium** impact and **12.50%** were ranked of a **low** impact.

The differentiation between web and mobile applications is reasonable due to the new technologies entering the market. Vulnerabilities are not only identified on the source code, but also on the security procedures and technologies deployed by the mobile operating systems.