Espion Insights

Top Security Controls For Organizations

bsi. | espion
A BSI Professional Services Company

Introduction

The rapid increase and reliance on revenue generating online platforms is putting ever increasing pressure on organizations to govern and protect their externally facing information assets, including customer and credit card data. As the volume of online platforms grow, organizations are finding it more difficult to understand what systems they have, if systems and data are secure, and what controls are in place to effectively manage the risk of operating online.

This paper highlights the importance of the implementation of effective security controls to increase you organization's security posture.

Overview

Espion, expert in managing and securing business information, conducts hundreds of security assessments and penetration tests across a wide variety of organizations and business verticals. This unrivalled experienced provides us with unique insight into the current trends and statistics of information security postures spanning a broad range of organizations.

From careful analysis of historical assessment data, we have documented the top security controls your organization should have in place to protect the confidentiality, availability and integrity of your organizations critical systems and their underlying data.

What are Security Controls?

Before we examine the results of our sample it is important that we discuss security controls, what they are and the key success factors for effective implementation and management. Typically divided into four categories security controls cover:

- Physical controls
  - e.g. fences, doors, locks and fire extinguishers;
- Procedural controls
  - e.g. incident response processes, management oversight, security awareness and training;
- Technical controls
  - e.g. user authentication (login) and logical access controls, antivirus software, firewalls;
- Legal and regulatory or compliance controls
  - e.g. privacy laws, policies and clauses.

These controls ensure that security incidents - where possible – are detected, prevented and if an incident does occur that it is resolved as quickly as possible. The correct design, implementation and management of security controls, deployed throughout the organization, provide assurance to organizations that exposure to security incidents are reduced to an acceptable level.

While it is true that security controls are deployed in most organizations, they can be poorly designed and incorrectly managed, resulting in ineffective and inefficient operation. Consequently, poorly implemented security controls do not reduce risk to an acceptable level and therefore are of very little value to an organization.

Top Security Solutions to Increase Your Organization's Security Posture

To show the criticality of missing or poorly designed security controls which can potentially lead to the introduction of some of the most severe security vulnerabilities, we used all of the security assessments and penetration test results we conducted in 2015 as a sample and analyzed the results.

Furthermore, we illustrate how organizations can implement key security solutions to significantly improve the security posture of their externally facing infrastructure and applications, reducing the risk of attackers compromising critical IT assets, applications and data.

The Results:

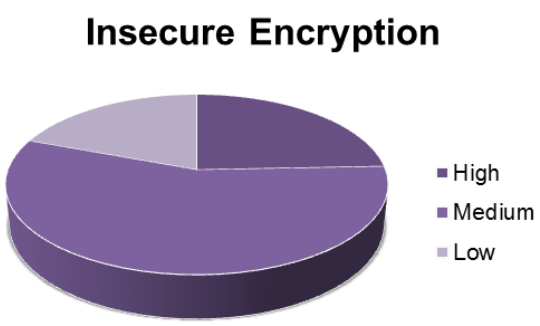
1. Strong Encryption

From the sample, it is clear that organizations are relying on out of date and insecure versions of encryption to protect the transmission of client server traffic, such as personally identifiable information (PII), financial data and credit card information.

In the wake of recent disclosed vulnerabilities discovered within SSL and TLS, (POODLE, BEAST, DROWN etc.) it is well documented that little to no reliance can be placed on older versions and ciphers.

These vulnerabilities directly compromise the core concept of encryption, resulting in the compromise of the confidentiality of any encrypted traffic using these ciphers.

Since the release of these vulnerabilities the PCI-DSS council has confirmed that the continued use of SSL and TLSv1.0 will result in a “fail” when assessed as of June 2018, increasing the importance from both compliance and security perspectives.

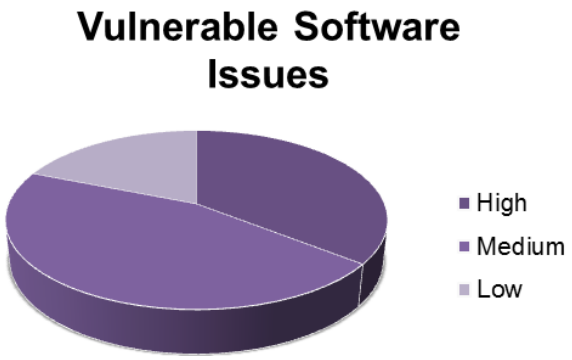


2. Patch Management

The rate at which vulnerabilities are being discovered and exploited in the wild has always been greater than the speed of response from the affected vendors. From our sample analysis it is apparent that without an effective patch management practice or patching plan, devices will continue to be exposed to known security vulnerabilities.

Over 700 of the vulnerabilities identified in the last year were related to out of date software or devices utilizing software which is no longer supported. This number of findings represents 29% of all issues discovered in the last year, indicating that strong patch management practices are not in place in many production environments.

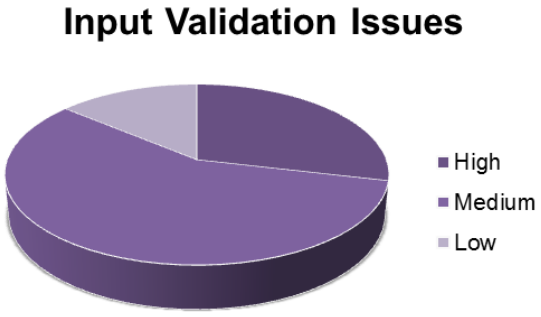
Of the vulnerabilities identified due to lack of effective patching controls, 36% of these were classified as “high risk” and introducing dangerous vulnerabilities into production environments, which could be avoided with an effective patch management practice.



3. Validating and Sanitizing Application User’s Input and Output

Web applications perform multiple roles for an organization, ranging from static content to providing the main revenue stream. Web applications are becoming more and more complex and most applications of value to an organization handle customer input in one way or another. This can vary from search and login functionality to the submission of payment and personal information.

Typically, user input is sent to the web server hosting the application and processed or stored by the application server or database server in the back end. Allowing user input to directly interact with these systems can allow an attacker to submit malicious input which is then processed by the application resulting in critical vulnerabilities such as SQL Injection or Cross-Site Scripting.



Input validation controls detect unauthorized user input before it is processed by the application. These typically include establishing strong validation patterns and output encoding.

This ensures only authorized input is allowed to be processed by the application and that any input provided by a user is converted into a “safe” form and not executed as code within the browser.

These solutions are often difficult to implement correctly as input validation and output encoding must be performed consistently throughout a web application.

Given the complexity of today’s applications and the wide variety of input fields, this task becomes increasingly more difficult.

While issues relating to a lack of input validation represent only 5% of the issues we discovered throughout the last year, overall they account for 25% of the high risk vulnerabilities discovered.

It is evident that while these issues may not be as prevalent as patching related vulnerabilities, when discovered they represent a huge security threat to an organization.

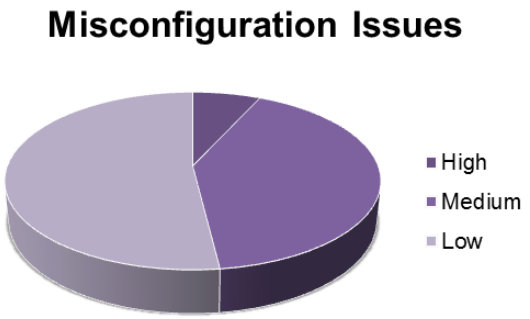
4. Securing Servers

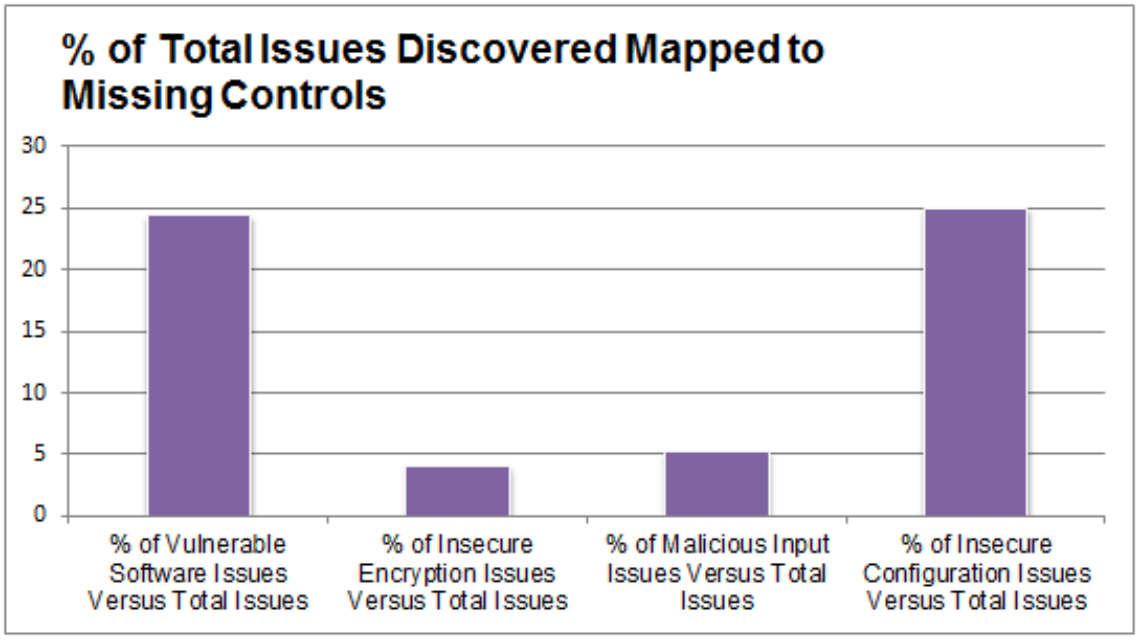
Misconfiguration of security controls on both infrastructure and application layers can lead to a large number of vulnerabilities being unnecessarily introduced into production environments. This is typically due to the lack of a server securing (“hardening”) procedure or maintenance plan for both infrastructure and applications.

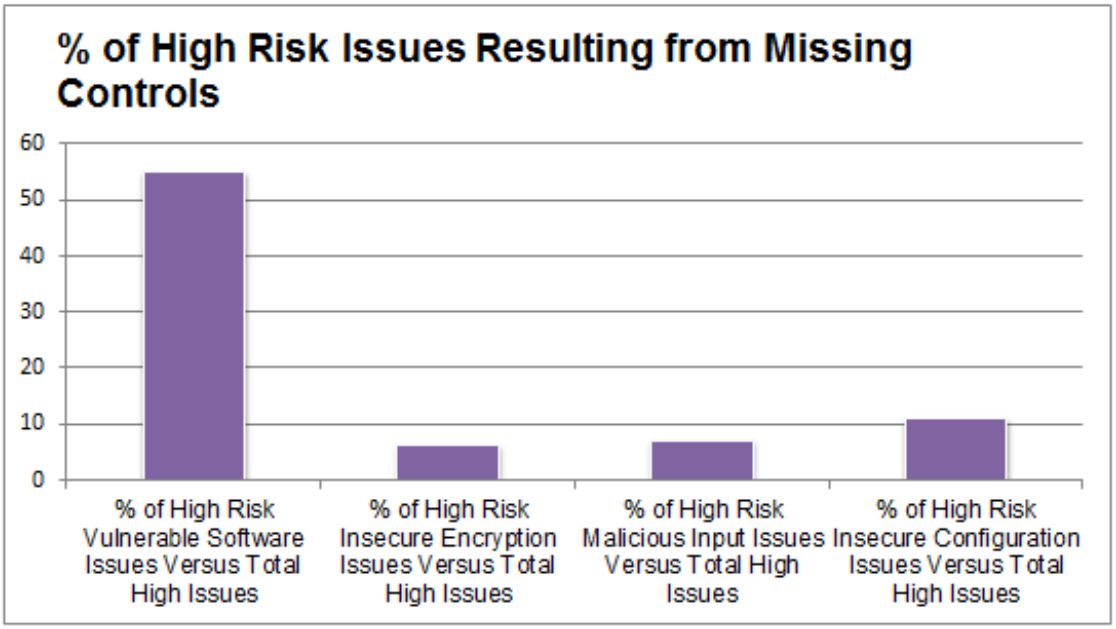
Consistently securing and hardening devices is essential for an organization with a externally facing server estate. The existence and adherence to these procedures ensures that all externally facing assets are secured and hardened consistently and any variances from this standard are documented and approved.

We discovered that 25% of all misconfiguration issues recorded were directly related to a lack of server hardening which represents 11% of all high issues discovered.

From our analysis, a common issue introduced through a lack of security hardening is exposing unnecessary ports and services to the Internet. This issue increases the attack surface of a device for an attacker and while controls such as strong input validation may be in place throughout an application sitting on this server; these controls are completely bypassed if SQL services are directly available to Internet borne attackers. Taking this example into account, it is clear that without correct server hardening, it is possible for an attacker to bypass critical security controls.







Critical Factors for Solution and Controls in Improving your Security Posture

As previously outlined, it is often the case that security controls, like the ones outlined in this paper, exist within an organization but may not be designed or operating effectively.

In this section we highlight some of the critical factors in identifying, introducing and maintaining security controls, which as an organization continues to grow and evolve, are essential in ensuring the success of an organization's security controls.

Real Solutions Are Long Term

Security Assessments by their very nature are "point in time assessments" of an existing server infrastructure and application security posture. Solutions from these assessments are often issue focused – targeting the symptoms of the problem but not necessarily the root cause.

A missing patch or vulnerability may be identified during this assessment but the same issues could be introduced back into the environment if the next iteration of patches are not applied to the affected system. This results in a never ending cycle of issues – and the organization ultimately loses. It is also important to note that while these top solutions may seem straightforward and basic, according to Verizon's Data breach Investigation Report [1], in 60% of breaches reported, attackers are able to compromise an organization in minutes. This shows that the majority of successful breaches are following "the path of least resistance" and with that timeframe in mind are simple to execute. These kinds of vulnerabilities are almost introduced to an organization through these missing controls.

Espion assists clients in identifying these issues, and more importantly their root causes, developing detailed remediation plans to ensure organizations can apply long term strategic improvements rather than short term tactical fixes.

Integrating Security as Your Organization Grows vs. Retrofitting Security

Often security concerns are not considered at the outset of most projects, with security controls "bolted on" at the end of the project lifecycle. It is important to note that this "retrofitting" security within an organization is vastly more expensive than investing in security from the outset.

The earlier a security culture and related practices are integrated within an organization, the greater the security posture of an organization. Organizations with an established, integrated security culture tend to have a much lower risk profile compared to those who 'fight fires' and attempt to add security at a later date.

Espion understands that knowing the root cause of vulnerabilities and effectively implementing security within an organization are two very different things. At Espion, we specialize in leading and developing project roadmaps to implement the necessary security controls and culture throughout an organization. We work directly with the organization to implement best practice security controls and develop alternative strategies to handle exceptions arising during the lifetime of the project.

Regular Assessments and Vulnerability Management Cycles

For an organization to truly understand their security posture, it is critical to perform regular security assessments and training. While these exercises can be performed internally, it is advantageous to have an independent third party perform these services, as this gives a true, unbiased view of an organizations risk profile.

Security assessments provide the following information to an organization:

- Quantifying and validating the "known knowns" – assessing controls and quantifying issues the organization are aware of
- Identifying the "unknowns" – issues the organization are not aware of

For an organization to truly benefit from these assessments, they must be carried out as part of a scheduled testing cycle and vulnerability management procedure. Without this, vulnerabilities may be addressed in a short term manner and little consideration is given to the wider impact of the root cause, its impact on the business and the full cost of

remediation. Often this results in the same vulnerabilities remaining in the production environment year in, year out.

In addition to performing assessments, Espion advises clients on how to establish a vulnerability management practice. This equips an organization with the means, documentation and procedures to effectively manage vulnerabilities and prevents a security team from being overwhelmed by assessment results while successfully managing the organization's IT security profile on an ongoing basis.

References

[1] - *www.verizonenterprise.com/ie/DBIR/2015/*

Espion

As an information security consultancy firm, we understand the value of data to your business and the serious implications of inadequate security controls.

Espion helps organizations secure their business data through our targeted set of services that identify and manage risk.

- Web-App Pen Tests
- Internal/External Pen Tests
- PCI-DSS Advisory
- Risk Assessment
- ISO27001 Advisory

Contact us to find out how we can help you secure your data.

Email: info@espiongroup.com

IRE: +353 1 2101711
UK: +44 845 050 1711
USA: +1 917 651 1783