Cost Effective Assessment of the Infrastructure Security Posture

G. P. Williams

IT Governance Ltd., United Kingdom, gwilliams@itgovernance.co.uk

Keywords: Infrastructure, attack surface, security posture, cost effective, assessment

Abstract

An organisation's security posture is an indication the countermeasures that have been implemented to protect the organisations resources. The countermeasures are security best practice that are appropriate to the organisations risk appetite and the business requirements. The security posture is defined by an organisations security policy and its mission statement and business objectives. Countermeasures come with a cost which should not exceed the value of the resources they are protecting and they should be effective, provide value for money, and a return on investment for the organisation Measuring how the organisations actual security posture relates to its agreed acceptable level of risk is a problem that is faced by organisations when looking at whether their countermeasures are effective and providing value for money and a return on investment. There are two methodologies that can be used.

1. Auditing – which is the mechanism of confirming that the processes or procedures agree to a master checklist for compliance
2. Assessing – is a more active, or intrusive, testing methodology to adequately assess your processes or procedures that cannot be adequately verified using a checklist or security policy

This paper investigates the surface attack area of an organisations infrastructure and applications examining the cases where the use of cloud and mobile computing have extend the infrastructure beyond the traditional perimeter of organisations physical locations and the challenges this causes in assessing the security posture. A review of the use of assessment methodologies such as vulnerability assessment and penetration testing to assess the infrastructure and application security posture of an organisation shows how they can provide identification of vulnerabilities which can aid the risk assessment process in developing a security policy. It will demonstrate how these methodologies can help in assessing the effectiveness of the implemented countermeasures and aid in evaluation as to whether there are provide value for money and a return on investment.

It is proposed that a long term strategy of using both methodologies for assessing the security posture based on the business requirements will provide the following benefits.

- Cost effective monitoring of the infrastructure and security posture.
- Ensuring that the countermeasures retain effectiveness over time.
- Responding to the continual changing threat environment.
- Ensuring that value for money and return on investment are maintained.

1 Introduction

Today organisations are facing a threat from cyber-attack, whether they are international conglomerate or a one man outfit, none are immune to the possibility of attack if there have a connection to or presence on the Internet. The attacks can take many forms from the Distributed Denial of Service through to targeted phishing emails; many attacks result in low tangible costs but can have high intangible costs to the targeted organisation such as lose of brand reputation and loss of business. Many small businesses have taken weeks to find their websites have been blacklisted by search engines as their site has been compromised and is now hosting malware.

Part of the reason for the increase in sophisticated attacks is the availability of toolkits that simplify the attack so that despite the sophisticated nature of the attack virtually anyone who is computer literate can use them.

Although attack sophistication has grown since the password guessing attacks in the early 1980's to the sophisticated Advanced Persistent Threat (APT) that is being seen today, the skill level required to launch attacks has dropped (see Figure 1) as the development of hacking toolkits and malware toolkits have increased given the script kiddie hack sophisticated tools with simple GUI interfaces. The hacking group Anonymous's use of tools such as the Low Orbit Ion Cannon (LOIC) available on sourceforge and github, enabled thousands of individuals who have no programming knowledge to take part in their orchestrated campaigns. The high profile of cyber-activity is encouraging increasing number of people to dabble with easily findable tools and scripts and many progress deeper into illegal activity.

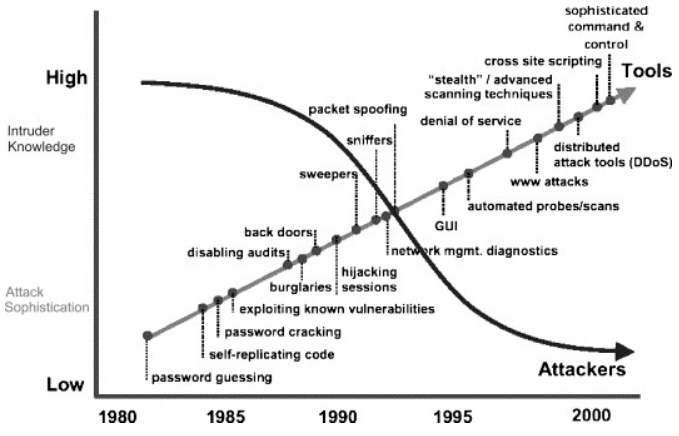

Figure 1: Attack sophistication vs. intruder technical knowledge [12]

To protect against such threats a prudent organisation will of implemement an Information Security Management System (ISMS), a set of policies concerned with Information security management or IT releated risks.

A key stage in the of implemention of ISMS is the risk assessment which identifies threats, vulnerabilities, control selection, likelihood, impact, risk determination, and control recommendations [7]. During the evaluation of risk an analyst will compare the level of risk determined to the risk criteria established by senior management. The risk criteria is a formal statement of the security posture the entity has determined to be acceptable.

For an ISMS to remain effective and efficient in the long term, adapting to changes in the internal organization and external environment therefore incorporates the typical "Plan-Do-Check-Act" (PDCA), or Deming cycle, approach, The best known ISMS is described in ISO/IEC 27001 and ISO/IEC 27002 and related standards published jointly by ISO and IEC. Another ISMS is Information Security Forum's Standard of Good Practice (SOGP). It is more best practice-based as it comes from ISF's industry experiences. Other frameworks such as COBIT and ITIL touch on security issues, but are mainly geared toward creating a governance framework for information and IT more generally. COBIT has a companion framework Risk IT dedicated to Information security. Although in the recently relased new version of COBIT, Rist IT has been cincorporated into the framework.

2 Infrastructure security posture

The security posture of a company is the accepted risk level to which a system or organization is exposed. In organizations that use formal certification and accreditation processes, the security posture is usually stated relative to its target risk profile. Most business systems aim to have a security posture of a low residual risk (after implementation of recommended safeguards).

An organisation's security posture is an indication the countermeasures that have been implemented to protect the organisations resources. The countermeasures are security best practice that are appropriate to the organisations risk appetite and the business requirements. The security posture is defined within an organisations security policy.

2.1 Attack surface area

Traditional a measure of exposure to the internet in the early days was the network perimeter and whilst the death of the traditional network perimeter has been heralded in many publications the more recent concept of the attack surface area is still very much alive and caters for mobile and cloud computing and the attack surface area can define a perimeter companies can use to better securing their networks and data. People are part of the company's attack surface and with bring/buy you're your device; people and their devices have further extended the attack surface and have become part of the perimeter.

As a measure of how vulnerable an entity on the internet is to an attack it the attack surface area which is defined as the exposure area that remains reachable and vulnerable to attack. It provides an indication of how much of the entities infrastructure is exposed to attackers and hence potential vulnerable. There has been work on quantifying the attack surface area; the most notable is Howard's Relative Attack Surface Quotient for Windows [5]

The attack surface area for an entity [1] consist of

- Hardware
- Software
- People

The network surface area contains all the intersections between the entities network and the internet, consisting of the gateways, routers, firewalls.

The software consists of the server operating systems and the server daemons /services running on that OS platform along with applications that provide functionality required to provide functionality, includes web applications

People consist of both internal and external users of an entities system can be weak points in the entities security; they are often the endpoint of various attack techniques, allowing attackers to bypassing implemented security countermeasures.

The traditional network perimeter has been weakening with the use of Virtual Private Networks to interconnect branches and individual across the internet and has been killed over with the rapid increase in use of mobile devices, the use of cloud computing and the very rapid increase in Bring Your Own Devices (BYOD). Although these technologies have put gaping holes through the network perimeter they still fit within the attack surface area model of network security.

2.2 Infrastructure

The focus of this paper it is on the IT infrastructure and for the purposes of the paper is defined [2] as a general term to

encompass all information technology assets (hardware, software, data), components, systems, applications, and resources of an entity, this is concentrating on two of the three legs of the attack surface area. In today's world of mobile, cloud and BYOD an entities infrastructure is now owned by multiple parties introducing a level of complexity for the management of the infrastructure not previous seen. In particular the use of BYOD has moved ownership of some of the infrastructure out of the organisations control into the hands of its employees.

2.3 Challenges of mobile, cloud and BYOD

Implementing controls for security on the infrastructure now involves contractual agreements and need for enforceable Service Level Agreements (SLA) with multiple parties, for an entity to test its infrastructure it needs permission not only from senior management but also from the other parties. One of the disadvantages of cloud computing is that commoditising of the services has led to the use of standardised terms and conditions from the providers, for example Amazon Web Services (AWS) has a specific set of terms and conditions that is supportive of organisations wishing to conduct vulnerability / penetration testing of their hosted services on the AWS platform. If a company has distributed its own mobile devices to employees then the testing can be included under the terms and conditions of the use of the device, however it must take into account an employee's right to privacy, In the case of BYOD they becomes a big problem in trying to access the controls, if an organisation has formalised a policy on the use of BYOD then it should contain terms and conditions about the security of the device that the user must agree to. Where an organisation has agreed to the use of personal devices they should be using one of the many products appearing to secure corporate data on a BYOD, a key feature of these management products is the ability to segregate personal and corporate data along implementing auditable security controls that are managed from the organisation IT department. A major security issue for organisations is where BYOD is being used on an ad hoc basis and is unauthorised and the organisation is relying on the employee to allow controls to be implemented or on the common sense of the employee in protecting corporate data.

3 Measuring security posture

Measuring how the organisations actual security posture relates to the organisations agreed acceptable level of risk is a problem that is faced by organisations when looking at whether their countermeasures are effective and providing value for money and a return on investment. There are two methodologies that can be used.

1. Auditing – which is the mechanism of confirming that the processes or procedures agree to a master checklist for compliance.
2. Assessing – is a more active, or intrusive, testing methodology to adequately assess your processes or procedures that cannot be adequately verified using a checklist or security policy.

3.1 Auditing

The security posture can be assessed by the use of auditing based on checklist approach. In an organisation the auditor would start the process by examining the current policies to see if they are implemented and enforced. These policies would maintain secure configuration of the system and would cover a wide range from patch management, anti-virus updates, access control via firewall configurations and logs monitoring, passwords and accounts management, critical systems backups, incident response plans and disaster recovery, change management procedures.

The auditor would then use these policies and procedures to form an audit checklist. Each key component of the SOHO will now be tested against the audit checklist to see if its configuration is as secure as it should be. Each checklist item was carefully chosen as the best control or method to test for a given risk possibly present in one of the components.

The checklist would need to cover the vulnerabilities covered in Open Web Application Security Project (OWASP) Top 10 project [9] and the SANS Institute top Twenty Critical Security Controls for Effective Cyber Defence: Consensus Audit Guidelines [11].

3.2 Methods of Assessment

Assessing vulnerabilities in the infrastructure can be done through two methodologies.

A Vulnerability Assessment looks for vulnerabilities in a system, whilst a Penetration Testing takes this a stage further and confirms whether vulnerabilities can be exploited.

Vulnerability Assessment	**Penetration Testing**
Identification of vulnerabilities in a system	Identification of vulnerabilities in a system
	Confirmation that a vulnerability can be exploited

Table 1: Comparison of Vulnerability Assessment and Penetration Testing

Vulnerability testing is a short, quicker process, effectively it can be a fixed length test based on the complexity of the infrastructure to be tested. It can provide an indication on how vulnerable the infrastructure maybe.

Penetration testing is a longer process that takes place after a vulnerability assessment involving a more manual intensive approach where identified vulnerabilities will be tested to see if they can be exploited and access to the infrastructure be gained. A penetration test will pose a higher risk to a production system than a vulnerability assessment as often an

exploit involved actual use of coding errors such as buffer overflow or command injection which could cause a system to become unstable.

Typically when conducting an infrastructure assessment, there are three typical forms of assessment conducted based upon the location of where the test is conducted from and which aspect of the attack surface is being tested such as hardware or the software. The three forms can be combined into a more comprehensive assessment.

External infrastructure	Test of public facing (on the internet) infrastructure, would examine the information each machine is presenting to the internet and whether the hardware or services running on the infrastructure have vulnerabilities
Internal infrastructure	Test of internal infrastructure, would examine the information each machine is presenting to the network and whether the hardware or services running on the infrastructure have vulnerabilities. Would also check on visibility between network segments. Wireless network infrastructure is often tested separately.
Application	Testing of the applications that are running on the infrastructure, the testing is typically external but may be internal.

Table 2: Three Typical Forms Of Assessment

There are a number of methodologies for conducting vulnerability assessments and penetration tests. The most common methodologies are the Open Source Security Testing Methodology Manual [4] and the OWASP testing guide which concentrates on application testing [8].

Vulnerability and Penetration testing of cloud systems is maturing sub-discipline with cloud providers and third parties offering specialist services. An important security control is segregation of duties and conflicts' of interest, having the cloud provider also provide security assessments is potential breaking these controls. An increasing number of third parties are providing cloud assessment services but the responsibility for conducting the test is with the commissioning company and they need to ensure that correct permissions have been gained before the assessment is started.

Although vulnerability assessment and penetration testing mirror the activities of an attacker when they try to attack a system there are a number of problems with the process.

Often a full penetration test cannot be conducted on a production system as the system is production disruption of the system in terms of possible outages, denial of service are not acceptable to the organisation.

In real life the attacker only needs to find a single vulnerability that can be exploited for an attack to be successfully, whereas for assessment purpose ideally we need to identify all the possible vulnerabilities in the system that can be exploited. This process can be very time consuming involving writing customised exploits which is an expensive process.

4 Cost Effective Assessment

The cost of assessing the infrastructure security posture is undesirable cost to organisations, as the assessment is measure of how the required security posture is being implemented. It is not directly attributable to the cost of implementing the control but additional cost in proving the level of the security posture.

Any security controls put into place must be proportional to the business objectives and provide value to the business. One of the difficulties in proving the Return on Investment (ROI) of a countermeasure is demonstrating its effectiveness; this is not just on the implementation but over the whole of its lifecycle. Quantitative risk analysis looks at the Annual Loss Expectancy (ALE) the value of the control can be expressed by looking at the ALE value before and after the implementation of the control as described below.

Value of countermeasure = ALE(without countermeasure) – Annualized cost (countermeasure) – ALE (with countermeasure)

The effectiveness of a countermeasure can be measured by looking at the how effective the countermeasure has been in reducing the risk of a vulnerability by comparing a vulnerability assessments before (baseline) and after its implementation.

For an assessment methodology to be cost effective it must provide value to the organisation by giving meaningful results at an acceptable cost. Regular vulnerability assessment and penetration testing can provide a means to measure the effectiveness of security and over a period of time will provide a measure of the performance of the security.

Continuous assessment is required, as what is secure today may not be secure tomorrow, the security posture must be assessed regularly, this is part of the PDCA cycle of an ISMS, an expensive assessment strategy can unnecessary inflate the cost of the information security function for an organisation.

The business requirement for the assessment is to obtain the required level of evidence from the assessment process to meet the organisations requirements at the lowest cost.

5 Discussion

In order to provide a cost effective assessment of the infrastructure security posture for an organisation they will need a mature ISMS where the requirements and expected outcomes of an assessment process are well understood by the organisation.

There are two methodologies that can be used by organisations for the assessment of the infrastructure security posture.

1. Auditing
2. Assessing

Auditing is a well understand method that organisation are already using internally and experience of using external auditors. It can be performed repeatable with consistent results. A disadvantage of auditing as an assessment methodology for security posture is the process can be 'cumbersome' when audit checklists are not available, or poorly prepared, the following disadvantages can happen and should be taken into consideration:

- Checklists can be restrictive if used as the auditor's only support mechanism;
- Generic checklists, which do not reflect the specific organisational management system, may not add any value and may interfere with the audit;
- Poorly prepared checklists can slow down an audit due to duplication and repetition;
- The focus of the checklist may be too narrow in scope to identify specific problem areas.

Assessing by either vulnerability assessment or penetration testing is a more effective method it is more responsive to the changes within the threat landscape and more accurately mimics the actions of threat agents on the infrastructure. Both methodologies require specialist knowledge in order for them to be effective. Although tools exist that can undertake automated vulnerability analysis the results require specialist skills to interpret them. Although many IT departments may be able to use the automated tools, the results from these scans will not necessarily provide valid evidence.

A full Penetration test is a lot more expensive than a vulnerability assessment provides additional information in terms of prove of an exploit exists that can be take advantage of a vulnerability it cannot give a guarantee that a system is secure. In determine whether a penetration test or a vulnerability assessment is cost effective consideration of the benefits of the extra evidence that can be obtained from having a full penetration test conducted compared with the evidence from a vulnerability assessment needs to be made with specific regards to the organisations business requirements.

It has been proven by the US Department of State that concentrating on the top twenty controls can give a 94% reduction in measured security risk [6]. Organisations concentrating on the top 20 information security controls will give the most significant return on investment. An assessment strategy based on measuring these controls will be the most cost effective assessment providing this meets the business requirements of the organisation.

For non-high risk organisations the most cost effective strategy for measuring the infrastructure security posture would be based on a regular vulnerability assessment augmented with a penetration test when specific high risk vulnerability as judged by the acceptable risk criteria approved by senior management, however for high risk organisations such as government or banking they will need a more in depth assessment strategy based on the use of penetration testing is likely to provide the required level of evidence.

6 Conclusion

The assessment of the infrastructure security posture does not lend itself to the use of auditing using a checklist approach. Although the comparative cost of conducting an audit may be lower the quality of the evidence and the likelihood of meeting the business requirements

The use of an assessment methodology using vulnerability assessment and penetration testing rather than an audit for assessing the security posture of the infrastructure is a more cost effective methodology to ensure the whole attack surface is tested.

As the threat environment is not steady state system the assessment methodology is better at responding to the changes in the threat landscape.

For non-high risk organisations the best strategy for measuring the infrastructure security posture would be based on a regular vulnerability assessment augmented with a penetration test when specific high risk vulnerability as judged by the acceptable risk criteria approved by senior management.

The benefits of such an assessment strategy will be:-

- Cost effective monitoring of the infrastructure and security posture
- Ensuring that the countermeasures retain effectiveness over time
- Responding to the continual changing threat environment
- Ensuring that value for money and return on investment are maintained

An important factor in ensuring an assessment is cost effective is to ensure that the recommendations in any assessment are implemented and the report is not treated as tick in ISMS checklist to say an assessment has been conducted.

References

[1] J. Carr, "Inside Cyber Warfare: Mapping the Cyber Underworld," Reilly publishing

[2] M. Gregg, D. Kim. "Inside Network Security Assessment: Guarding Your IT Infrastructure" Published by Sams.

[3] S. Hansman, R. Hunt, "A taxonomy of network and computer attacks" Department of Computer Science and

Software Engineering, University of Canterbury, New Zealand

[4] P. Herzog, “Open Source Security Testing Methodology Manual “ (OSSTMM) http://www.isecom.org/research/osstmm.html

[5] M. Howard, “Fending Off Future Attacks by Reducing the Attack Surface” Feb. 2003

[6] J. Streufert, “Measure More, Spend Less On The Way To Better Security” US Department of State. November 12, 2009

[7] NIST Risk Assessment methodology

[8] OWASP Testing Guide https://www.owasp.org/index.php/Category:OWASP_Testing_Project

[9] OWASP Top Ten Project https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[10] Penetration Testing Amazon Web Services http://aws.amazon.com/security/penetration-testing/

[11] SANS 20 Critical Security Controls http://www.sans.org/critical-security-controls/

[12] “Attack sophistication vs. intruder technical knowledge.” Computers & Security, Volume 24, Issue 1, Pages 31–43, February 2005