PwC Poland

Penetration tests

Our approach to penetration testing in the cloud

Penetration test of Internet facing infrastructure

The Internet facing infrastructure can often be the main point of interest to the cybercriminals and is frequently the first vector of attack. It is crucial to eliminate potential vulnerabilities in the Internet facing infrastructure, as it may create further opportunities for compromise of resources and assets. Performing regular penetration tests can greatly decrease the risk of a security breach and can help better understand the overall security posture of the infrastructure.

Our approach

- Black-box and grey-box testing
- Fuzzing and identifying potential attack vectors
- Manual verification of identified vulnerabilities

Penetration test of an internal cloud or hybrid infrastructure

This part of test assumes the presence of an attacker within the internal network of the company. Wether the infrastructure is cloud-based or a hybrid configuration is in place, the goal of the test is to identify the vulnerabilities within the internal network and assess the possibility and impact of a potential, successful exploitation.

Our approach

- Penetration testing within the internal network
- Identification of key business systems and security mechanisms
- Assessing the possibility of using identified vulnerabilities to get unauthorized access to restricted resources

Manual review of cloud configuration and key, selected hosts

During this part of the assessment, we verify the security configuration of the cloud subscription, as well as the configuration of selection of hosts that is critical from the business perspective. We verify the controls against the industry's cloud best practices and standards. The manual review of access controls, implemented logging and monitoring mechanisms and encryption is a great way not only to defend against a remote attacker, but also to protect against an insider threat.

Our approach

- Verify security mechanisms in place and cloud configuration against industry's best practices
- Thorough inspection of critical, key systems and hosts

Penetration test of Internet facing infrastructure

During this part of the assessment we use a vast variety of hacking techniques and tools aimed directly at identified vulnerabilities in the Internet facing network. By doing this, we simulate real life system exploitation attempt.

- **Penetration testing** targeting the external IP addresses
- Analysis of users and administrators **access control system**, with focus on reliability of authentication and authorization methods (preventing privileges escalation)
- Testing the resilience of network protocols to **any manipulation over parameters** that ultimately may lead to escalation of privileges or Denial of Service attack, which results in network services breakdown or significant problems with accessibility
- Verification of the methods and techniques used for **data storage on the server side**, with particular focus on confidential data, as well as adequacy of logical safeguards that prevent from their disclosure
- Verification of selection and configuration of **cryptographic methods**
- Evaluation of the **administrative accounts enumeration** possibility
- Testing the resistance to **unauthorized configuration change** attempts
- Testing the resistance to **brute force password guessing** attempts

Penetration test of an internal cloud or hybrid infrastructure

The scope of this task covers penetration testing of the infrastructure, that is only accessible from the internal network. For this, we assume we are provided with some basic access level to the network, e.g. by the means of IPsec tunnel.

- Performing **penetration testing** of the resources indicated in the scope of work
- Identification of key **business systems**
- Analysis of the **security mechanisms** of the identified business systems
- Assessing the possibility of using identified vulnerabilities to get **unauthorized access** to restricted resources
- Attempting to explore the **resources shared on network drives**
- Verificatoin of the implemented **encryption of the protocols** (encryption in transit and at rest)
- **Guessing passwords** to the system accounts, assuming they are not complex enough
- Other adequate **logical and technical safeguards** providing security with assessment of their required efficiency.

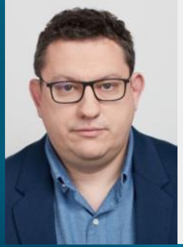
Manual review of cloud configuration and key, selected hosts

This section of the assessment covers review of the cloud configuration and security setup. To perform these tasks we will need an account with appropriate role assigned within the cloud subscription, that will allow us to log into cloud platform and review its' configuration.

- Checking the **security configurations** and **access controls** (Multi-Factor Authentication, user' permissions and roles)
- Verifying whether **security policies** are set and are the subscriptions **compliant** with the policies
- Reviewing the configuration against **cloud's best practices** (how the resources communicate with each other, are they using hardcoded credentials or security groups, how are the hosts accessed from outside the cloud network)
- Verifying whether **threat protection** is enabled on all possible resources and is it configured properly
- Identifying if sufficient level of **logging and monitoring** is set
- Checking **data encryption** in transit and at rest and verifying whether data is backed up in a secure way
- Manual analysys of the key resources' configuration, such as crucial **virtual machines** and **databases**

Contact us

and learn more



Szymon Sobczyk

PwC Senior Technology Leader
+48 519 504 525
szymon.sobczyk@pwc.com

Łukasz Żółtowski

PwC Manager
+48 519 507 557
lukasz.zoltowski@pwc.com

Microsoft Partner

2017 Partner of the Year Finalist
Public Sector: Microsoft CityNext Award

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. At PwC, our purpose is to build trust in society and solve important problems. PwC is a network of firms in 157 countries with more than 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.pl.