Microsoft Azure Security Assessment

SecWise

Microsoft

An expert 3-day security assessment focusing on your Azure Iaas/Paas environment to really secure your Azure public cloud.

Threats have become more sophisticated and increasingly tailored to the weaknesses of targets. To help ensure that an enterprise can respond appropriately, security should be applied at the onset of an enterprise's infrastructure design. Even if this infrastructure runs in the Microsoft Azure public cloud.

What's your security posture?

The security landscape has changed dramatically over the past three years and we have identified that many technologies are not prepared to deal with these new threats. Automated malware detection and forensics often occur too late—after the breach—and it can take months before one notices they have been compromised.

In response to these constantly evolving threats, you need to make sure that your Azure infrastructure security design combines innovative security solutions with security best-practices. These features harden identity, data, and hosted applications against common attacks, and help you respond more effectively to the targeted breaches when they happen.

Great, but what can I do?

SecWise offers a Azure Security Assessment that helps you understand the potential security benefits and its relevance for **your Azure** IT environment. This assessment will help you plan for the future through a TO BE roadmap and security recommendations. You will be provided with an overview of the current threat landscape, and we will assess your current Azure cloud security posture. After this 'AS IS' assessment we will design a 'TO BE' Azure security architecture to fill the security gaps and thus to protect your cloud environment, together with a phased roadmap for implementation.

Benefits

Understand the security threats of today and how to **secure your Azure workloads.**

Prioritize the implementation of the key features and scenarios **based on cloud cyber best-practices and business context**.

SecWise NV

Securing your Digital Transformation

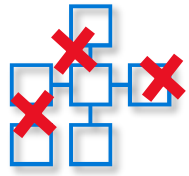
Gaston Geenslaan 11, B4

3000 Leuven

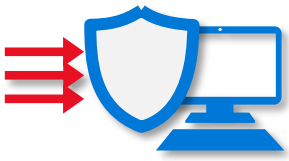
www.secwise.be

Addressing attacker's threats requires an innovative approach

KNOW THE ATTACKER'S ECONOMIC MODEL



BREAK THE ATTACK PLAYBOOK



FUTURE-PROOF AZURE DEFENSE DESIGN

What can you do?

SecWise offers an Azure Security Assessment that helps you understand the current cyber security threat landscape and maps this to you current Azure infrastructure cyber security defenses. This assessment will help you through a 'fit-gap' analysis of your '**AS IS**' defense versus **a future proof 'TO BE'** cyber security defense.

Objective of the assessment:

- Overview of the current cyber security threat landscape
- FIT-GAP analysis on your current 'AS IS' Azure cyber defense versus security gaps & risks
- Recommendations and 'TO BE' Azure security architecture design based on the Microsoft Defender for Azure eco-system and/or third-party tools
- Personalized roadmap proposal based on risk prioritization

Azure Security Assessment Offer

- ✓ 3-days
- ✓ Senior Azure Security Architect
- ✓ 3.000 € in total (excL.VAT)
- ✓ Output: Fit-gap analysis, with TO BE recommendations & cyber security design
- ✓ High-level roadmap based on Risk priority

Topics covered: Authentication & access control: which user accounts are defined as "owner" of the full Azure subscription (delegation) or have privileged rights? Is MFA in use? etc..
Network security: firewall / WAF config, are internal projects isolated at the network level (network security groups), is the connection between on-prem and cloud secured (express route, site2site VPN, ...), are individual services well insulated or secured at network level (Bastion instead of RDP to VMs, storage / databases not accessible from the internet (or with IP restrictions), ...etc
IAAS/PAAS security: traditional measures such as AV, WD ATP on server level, hardening, etc. Also for VM's (both Windows and Linux); is Docker used and does that require specific hardening? ... etc.
Encryption of data-at-rest and in transit: VM disks, databases, storage, etc
Auditing & compliance monitoring - is Azure Security Center already in use? Or another tool for this?
Threat monitoring at server level.

Take your first steps towards a more secure future! Contact us: cloudsecurity@secwise.be