

nixu
cybersecurity.



Microsoft

Cloud security

Microsoft Cloud Security
assessments



Trusted go-to partner for cybersecurity services

Vision:
Keeping the digital
society running



Mission:
Be the best workplace
For cybersecurity
specialists



400+

Cybersecurity
specialists



11

 Locations

Finland, Sweden,
Netherland,
Denmark and
Romania



Cybersecurity services
from board decisions to
deep forensic investigations

Founded in

1988

publicly listed

2014



98%

of our clients
recommend Nixu

Comprehensive Cloud Security

Security Strategy



Microsoft Azure



Amazon Web Services



Google Cloud Platform



Alibaba Cloud

Security Governance



Threat modeling



Platform security



Privacy



Secure architecture



Code security



Vulnerability Management



Security Monitoring (Nixu SOC)

nixu
cybersecurity.



Security assessment for Microsoft Cloud services

Analyze the overall security posture to identify risky configurations, findings from best practices and get propose for actionable mitigations



Azure platform

Security assessment covers individual Azure resources and resource types. Each resource is analyzed against known best practices and hardening guidelines.



Azure AD

Security assessment covers Azure AD tenant-level security controls and ensuring access management is properly implemented.



Microsoft 365

Security assessment covers Microsoft 365 tenant security controls and analyzed against known best practices and hardening guidelines.



Our understanding of the situation

Get an assessment on your Microsoft cloud solution security with prioritized findings and recommended actionable mitigations.

Challenges

Situation & needs

- Business is becoming more and more dependent on digitalization and on cyber
- **Business is moving more and more to the Cloud Services**
- Unclear status of Cloud security
- The cyber threats expose significant risk to critical business data
- **Need to understand the current cloud security posture**
- **Need of security check in the SDLC projects (SecDevOps)**

Service offering

Value proposition

- ▶ Get control of your cloud security posture and feel confident
- ▶ **Know where you stand and get a full view of your Cloud security with findings**
- ▶ Mitigate the cyber risk for your Cloud and make your critical business applications and data more secure
- ▶ **Get an actionable recommendations of your cloud security risk**
- ▶ Plan and prioritize your security improvement based on best practices

Solution & Outcome

- **Assessments result of your Microsoft Cloud Service**
- Security assessments based on:
 - Microsoft best practice
 - Nixu best practice
 - industry best practices
- **Security findings with severity level**
- **Actionable recommendation mitigation actions**

Cloud security assessment in context



To whom, where and what?

Who is in need?



Typical audiences:

- Development and deployment teams
- Service managers for cloud services
- Service managers for infrastructure services
- Infrastructure & enterprise architects
- IT security and compliance
- IT operations team

Where is the need?



What to get?

Assessment result of security controls

Severity level of the findings

Recommended **actionable** mitigation



Nixu's methodology and deliverables



Security assessment method

The assignment steps with main goals and activities

Standard time span:
4 weeks



Workshops	Preparation	Kick-off	Analysis	Closure
Goals	<ul style="list-style-type: none">Project scope, approach and practicalities agreedDocuments for review available for Nixu	<ul style="list-style-type: none">Information gathered from the CustomerData collected from scanning result	<ul style="list-style-type: none">Customer understands the scanning result and findings	<ul style="list-style-type: none">Customer understands the recommended actionable mitigations
Activities	<ul style="list-style-type: none">Review scope objectives and target outcomesPrepare workshop materialsReview required permissionsIdentify stakeholders	<ul style="list-style-type: none">Review architecture and design imperativesPerform technical scanning	<ul style="list-style-type: none">Review and verification of scanning results by expertIdentify possible changes to the environment	<ul style="list-style-type: none">Finalize the review and ensure findings are correctDiscuss whether continuous assurance, or follow-up meeting is requiredDeliver the outcome (report)
Deliverables	<ul style="list-style-type: none">Interview schedule	<ul style="list-style-type: none">Technical scanning	<ul style="list-style-type: none">Scanning result and findings	<ul style="list-style-type: none">Severity level of findingsRecommendationsReport

Report

Assessment result

- The security scanning is based on best practice.
- The scanning result are reviewed and verified by experts.
- The recommendations are defined as actionable mitigations

Report structure

- Introduction
- Background and architecture
- Assessment findings
- Top recommendations
- Audit data



Customer – Azure Security Assessment Confidential 11 (65)

4 Subscription Scan Results

4.1 Scope

Scope /subscriptions/78020cde-0dd8-4ac6-a6d4-21bac00fb343
SubscriptionId 78020cde-0dd8-4ac6-a6d4-21bac00fb343
SubscriptionName Dewired - MPN

4.2 Controls

4.2.1.1 Passed - Azure_Subscription_AuthZ_Limit_Admin_Owner_Count

Status Passed
Severity Medium

Recommendation There are 2 steps involved. (1) You need to remove any 'Classic Administrators/Co-Administrators' who should not be in the role. Please follow these steps: (a) Logon to <https://portal.azure.com/> (b) Navigate to Subscriptions (c) Select the subscription (d) Go to 'Access Control (IAM)' (e) Select the co-administrator account that has to be removed and click on the 'Remove' button. (f) Perform this operation for all the co-administrators that need to be removed from the subscription. (2) You need to remove any unwanted members from the Owners group. To do this simply run the command 'Remove-AzRoleAssignment -SignInName '{signInName}' -Scope '/subscriptions/{subscriptionid}' -RoleDefinitionName Owner'.

Rationale: Each additional person in the Owner/Contributor role increases the attack surface for the entire subscription. The number of members in these roles should be kept to as low as possible.

Description Minimize the number of admins/owners
Investigate: [Ref SVR](#)

4.2.1.2 Verify - Azure_Subscription_AuthZ_Justify_Admins_Owners

Status Verify
Severity Medium

Recommendation There are 2 steps involved. (1) You need to remove any 'Classic Administrators/Co-Administrators/Owners' who should not be in the role. Please follow these steps: (a) Logon to <https://portal.azure.com/> (b) Navigate to Subscriptions (c) Select the subscription (d) Go to 'Access Control (IAM)' (e) Right click the co-administrator account that has to be removed and click on the 'Remove co-administrator'. (f) Perform this operation for all the co-administrators that need to be removed from the subscription. (2) You need to remove any unwanted members from the Owners group. To do this simply run the command 'Remove-AzRoleAssignment -SignInName '{signInName}' -Scope '/subscriptions/{subscriptionid}' -RoleDefinitionName Owner'.

Rationale: Accounts that are a member of these groups without a legitimate business reason increase the risk for your subscription. By carefully reviewing and removing accounts that shouldn't be there in the first place, you can avoid attacks if those accounts are compromised.

Description Justify all identities that are granted with admin/owner access on your subscription.
Investigate: [Ref SVR](#)

Nixu Corporation / 2020 nixu

Security control status

Severity level

Recommended
actionable mitigation



Service levels & Additional services

Microsoft Cloud Security Assessment



Nixu service levels



Components			
Microsoft Cloud Security Assessment	Azure platform	Azure AD	Microsoft 365
Interviews	✓	✓	✓
Architectural reviews	✓	✓	✓
Technical configuration analysis	✓	✓	✓
Security scanning			
Microsoft Best practice	✓	✓	✓
Nixu Best Practice	✓	✓	✓
Report			
Security control status	✓	✓	✓
Severity level assessment	✓	✓	✓
Recommended actionable mitigations	✓	✓	✓

Additional and other services

Services that can be added or combined with our assessments

Additional services

- Cloud Security Advisory
- Code Audit
- Application architecture review
- Penetration testing
- Microsoft 365 Sensitive Data Analysis
- Component deep-dive security analysis

Other Services

- Red teaming
 - Red Teaming against Azure AD access management controls
- Security monitoring (SOC) capabilities
 - Starting with Defender ATP, Sentinel and MCAS
- Shadow IT Discovery
 - Provides insight on cloud usage, security objectives and requirements



Contact:
Nixu Cybersecurity
sales@nixu.com

 [nixu](#)

 [@nixutigerteam](#)

 [company/nixu-oy](#)

www.nixu.com

