dionach

Ensure you meet your Microsoft Azure and M365 security responsibilities

A case study looking at a recent Microsoft Azure and 365 security review engagement

dionach

Penetration Testing
Case Study

Contents

01. Background

Cloud computing is of growing interest across different size companies around the globe. Microsoft Azure is one of the most popular solutions for enterprise, due to its deeply-integrated Azure and 365 cloud services, enterprises can rapidly build and manage complex infrastructure to support key services. Since the Azure cloud platform offers more than 200 products and services this allows organisations to use tools and technologies they trust and are already trained to do so.

Many organisations migrate on-premise applications and data from their local data center to public cloud infrastructure to take advantage of benefits such as greater cost management, redundancy and security of systems and data. Azure comes with a lot of security tools and options which can be customised and configured, however with that flexibility comes the potential to introduce weaknesses and misconfigurations.

02. What is an Azure and 365 Security Review?

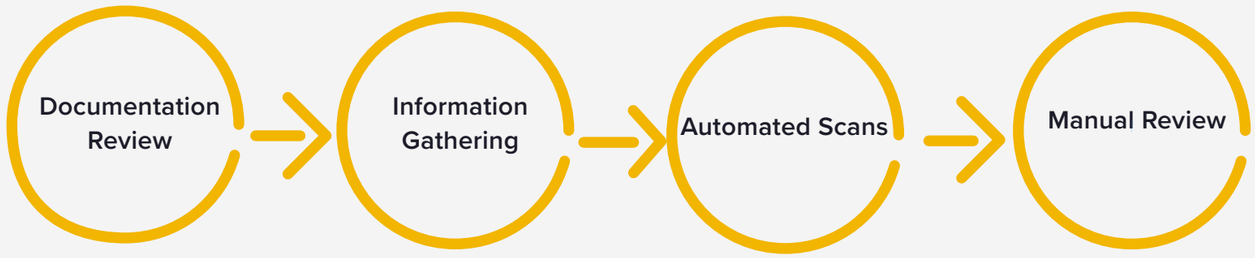
A Microsoft Azure and 365 security review is a security assessment that aims to identify any weaknesses associated to the cloud environment configuration that poses a risk to the organisation and its data. The assessment is conducted using a combination of automated tools and manual inspection of the cloud environment using read-only accounts with full access to the environment. The Dionach consultants will review the configurations and settings of all services in use against vendor and industry best practices. Reviews can also be carried out against security benchmarks such as those provided by the Center for Internet Security (CIS). During the review Dionach consultants will be collaborating with the organisation's technical staff to better understand the implementation and design of the cloud infrastructure environment.

Benefits of an Azure Security Review

A Microsoft Azure and 365 security review provides a complete review of the Azure infrastructure aiming to identify misconfigurations, lack of best practices and secure configurations. Areas of non compliance for certain regulations, such as GDPR, will also be identified allowing organisations to remediate identified weaknesses before they are exploited.

The Process

Microsoft Azure and 365 cloud infrastructure configuration designs and services in use are different for each organisation so the exact technical approach to each environment is different.



An Azure Security review follows a methodical process which involves the following the phases:

Documentation Review

- Security achitecture documents and network diagrams
- Configuration standarts
- Vendor and security best practices
- Security benchmarks

Information Gathering

- DNS, WHOIS, email, metadata
- Ineternet search, search engine queries
- Leaked credentials
- Threat modelling

Automated Scans

- Cloud security scans
- Compliance scans against security benchmarks

Manual Review

- Identify and access management (IAM) review
- Data security review
- Network security review
- Operational security review

Firstly, Dionach will review all relevant documentation related to the Azure and Microsoft 365 cloud environment. The next step is to perform information gathering against publicly available information on cloud resources that could be used in targeted attacks. This would include information, such as DNS records, document metadata and leaked credentials that could be used in gaining access to the cloud environment.

Once all relevant information is gathered, work will commence on the Azure and Microsoft 365 automated and manual security assessment stage. This would start by running a variety of automated scans using a combination of inhouse and third-party tools and scripts which utilise Microsoft Graph API. Following the automated scans, the Dionach consultant would then focus on manual review of the cloud environment in order to identify misconfigurations and security vulnerabilities. As part of this phase, the scan results from the previous phase will be manually reviewed to ensure no false positives are reported.

A manual review will be carried out against vendor and security best practices, and misconfiguration typically exploited during penetration tests or red team engagements. The review will take into consideration the organisation's business requirements and design decisions, including security configurations that are not checked by automated tools.

Typically, the majority of time in a cloud assessment engagement is used during the manual review phase, giving the consultant greater flexibility in focusing the security review in areas of concern for the business. Ultimately giving the organisation a higher standard of assurance.

dionach

Your report

When the Azure and Microsoft 365 security review is complete, Dionach will provide a report that includes:

· Executive summary for senior-level management.

· Exploitation paths, showcasing privilege escalation attacks.

· Details of vulnerabilities identified, along with proof-of-concept examples enabling your IT team to fully understand the identified issues.

· Tailored bespoke technical recommendation for fixing or mitigating the discovered vulnerabilities.

03. Real World Example

Context

The medium size organisation approached Dionach requesting a security review of Microsoft Azure and 365 cloud environments. The organisation has recently migrated to a hybrid cloud environment and wated to ensure that no misconfigurations were introduced as part of the migration process.

Exploitation and Privilege Escalation Path

Dionach initially performed the information gathering stage of the Microsoft Azure and 365 security assessment, running automated tools, reviewing scan results and identifying misconfigurations and weaknesses, including misconfigurations of conditional access policies and Azure role-based access control (RBAC).

During the informational gathering phase, a number of leaked credentials belonging to the organisation employees were identified. All of them were verified against Azure and Microsoft 365 login portals. Even though the majority of the credentials were found to be invalid, one user (name.surname@example.com) credentials were found to be valid in a sense that it was possible to login to the organisation's cloud environment.

During the review it was identified that no conditional access policies were created and enforced. Conditional access policies allow organisations to set specific conditions for granting access to resources. These policies can be used to ensure that only authorised users are able to access specific resources, and that they are only able to access them from specific locations or devices. Since no multi factor authentication across all user and administrative accounts conditional access policy was enforced, this misconfiguration allowed Dionach to successfully login to Azure environment with the credentials found on the Internet.

As part of the automated and manual review phase the role assignments were reviewed of all users and service principals. It was identified that the user "name.surname@example.com" had the Application Administrator role scoped to the tenant. The Application Administrator role is a built-in Azure AD role which can create and manage all aspects of app registrations and enterprise apps.

Since the "name.surname@example.com" was found to have the Application Administrator role assigned, the next step was to review if there are any applications registered with overly permissive service principals assigned to them. Azure applications needing to authenticate to the tenant to perform actions use Service Principals, they work like users, and allow authentication to the tenant with an object id and a certificate or secret.

During the review it was identified that the tenant contained the "Example App" application which had a global administrator role assigned to its service principle. Since the "name.surname@example.com" user had an Application Administrator role assigned, it had administrative control over the "Example App" application, which allowed it to add a new secret for the application's service principle. The "name.surname@example.com" user could then authenticate to the tenant with the newly added secret as the "Example App" service principle and use the service principle rights as a global admin to escalate the user privileges to the global administrator.

04. Key Takeaways

Following the delivery of the Azure and Microsoft 365 security review Dionach arranged a meeting with the organisation to ensure knowledge transfer of the following key points as well as that the chain of vulnerabilities was sufficiently mitigated:

· Monitor password breaches for email addresses which contain organisation specific domains and ensure that users with leaked credentials change their passwords immediately. Additionally, consider reviewing the internet usage policy to ensure that a requirement stating organisational usernames and email address shall not be used on third-party websites is included.

· Review conditional access policies to ensure they follow best practices and that multi-factor authentication is enforced for all users and that no users are allowed to login to the environment and access corporate resources from untrusted devices and locations.

· Review roles assigned to users and service principles to ensure all of them provide only the necessary access following the least privilege principle.

· Carry out regular reviews of roles and their assignments as part of user access rights review procedures, mainly to ensure that users cannot combine specific permissions in order to escalate their privileges within Azure.

Contact Dionach

Dionach is an independent CHECK-certified and CREST-approved global provider of information security solutions. With a twentythree-year track record of delivering insight-led cybersecurity services to organizations worldwide, we are the ideal partner to strengthen your cyber resilience, mitigate risk and safeguard your most valuable information assets right across the enterprise.

We are proud to be ISO 27001 and ISO 9001 certified, a PCI Qualified Security Assessor (QSA) and one of just 22 companies worldwide to hold the status of PCI Forensic Investigator (PFI). This testifies to the industry-leading competence of our technical specialists and our dedication to achieving the highest possible standards in service delivery.

Over 200 public and private sector organizations worldwide currently entrust their cyber security to our expanding global team. For more information on Dionach and how we can assist your organization, please contact us via **www.dionach.com** or call and speak to one of our consultant representatives.

5. Our Services

Assurance

Information security assurance through penetration testing and social engineering

Compliance

Meet compliance requirements for standards such as PCI DSS, ISO 277001 and Cyber Essentials.

Response

Understand and limit breaches and mitigate the risk of potential future ones.

Healthcare

Dionach developed programmes that now form the basis of NHS Digital's Cyber Security Support Model. Dionach are the appointed supplier delivering the Data Security Assessment (Identify) along with the Cyber Risk Framework Workshop (Embed).

Dionach Oxford

Unipart House
Garsington Road
Oxford
OX4 2PG

+44 (0)1865 877830

Dionach Glasgow

4th Floor
94 Hope Street
Glasgow
G2 6PH

+44 (0)141 488 3694

Dionach Manchester

Colwyn Chambers
19 York Street
Manchester
M2 3BA

+44 (0)161 713 0176

www.dionach.com